Uso de Virtualização de Recursos Computacionais na Administração de Redes

Guilherme Piegas Koslovski, Márcio Parise Boufleur, Andrea Schwertner Charão

[1]Laboratório de Sistemas de Computação (LSC)
Curso de Ciência da Computação – Universidade Federal de Santa Maria (UFSM)
Campus UFSM – 97105-900 – Santa Maria – RS – Brasil

{guilherm, boufleur, andrea}@inf.ufsm.br

Resumo. *O uso de ferramentas de virtualização vem se tornando popular em ambientes distribuídos. A virtualização permite executar múltiplos sistemas operacionais em um mesmo computador hospedeiro, cada qual com sua própria visão da arquitetura física subjacente. Tal habilidade é vantajosa para um aproveitamento eficiente do hardware disponível, além de trazer benefícios do ponto de vista da administração de sistemas. Neste artigo, apresenta-se uma análise de trabalhos recentes que exploram tecnologias de virtualização em sistemas em rede, com ênfase nas ferramentas Xen e VMware, que são duas soluções de virtualização bastante utilizadas atualmente. Os resultados deste trabalho constituem subsídios para administradores de redes interessados em empregar ferramentas de virtualização.*

1. Introdução

A virtualização de recursos computacionais é um tema recorrente em trabalhos de pesquisa e desenvolvimento envolvendo diversas áreas da computação. A abstração oferecida pelas máquinas virtuais permite mapear recursos reais de uma mesma arquitetura às necessidades de diferentes sistemas e aplicações, contribuindo para a flexibilidade, a portabilidade, a interoperabilidade, a segurança e a gerenciabilidade de sistemas de *software*.

Em um ambiente virtualizado, as tarefas de gerenciamento, escalonamento e alocação dos recursos disponíveis são executadas por um Monitor de Máquinas Virtuais (MMV). Este monitor virtualiza o *hardware* existente, oferecendo uma interface individual para cada máquina virtual, permitindo desta forma uma execução transparente e independente de uma arquitetura específica.

A separação lógica proporcionada pelas máquinas virtuais pode ser útil para administradores que buscam a consolidação de seus sistemas, aproveitando ao máximo o *hardware* disponível. A virtualização pode proporcionar um sistema mais seguro que nos casos em que os serviços executam todos sobre o mesmo sistema físico, pois os monitores de máquinas virtuais (MMV) podem garantir acesso restrito ao *hardware*, de modo que cada serviço tenha acesso somente aos recursos de que ele necessita.

Dentre as soluções de virtualização mais populares atualmente, destacam-se Xen [Barham et al. 2003] e VMware [Sugerman et al. 2001], ambas voltados à arquitetura Intel IA32. O presente artigo apresenta um panorama de trabalhos recentes envolvendo estas duas ferramentas, de modo a prover subsídios para administradores de sistemas interessados em utilizar virtualização para gerenciamento de redes de computadores.

Este artigo está organizado da seguinte forma: na seção 2 descreve-se o funcionamento e as principais características de monitores de máquinas virtuais, apresentando-se também as características e funcionamento das duas soluções de virtualização estudadas. Na seção 3 discute-se o uso destas ferramentas de virtualização no contexto do gerenciamento de redes e sistemas distribuídos, ressaltando-se as vantagens e desvantagens de cada ferramenta. Na seção 4 traçam-se as considerações finais sobre o presente trabalho.

2. Monitores de Máquinas Virtuais

O conceito de virtualização foi amplamente pesquisado e utilizado no início da década de 70, permitindo o compartilhamento dos recursos computacionais dos grandes *mainframes* entre as máquinas virtuais existentes [Goldberg 1974].

Atualmente, além de obter um melhor aproveitamento do alto poder computacional dos computadores modernos, a virtualização é utilizada como uma forma de interligar tecnologias [Smith and Nair 2005]. De fato, os computadores atuais possuem diversos componentes de *hardware* e *software* que interagem fortemente. Neste contexto, a virtualização constitui uma solução capaz de garantir a interoperabilidade entre tecnologias, de forma que o *hardware* virtualizado, independente da forma de implementação, possa ser acessado através de uma camada de abstração oferecida por um monitor de máquinas virtuais.

Um monitor de máquinas virtuais (MMV) é um sistema responsável pelo gerenciamento e alocação dos recursos do sistema hospedeiro entre diversas máquinas virtuais. Através do MMV, os sistemas em execução sobre a arquitetura virtualizada podem ter acesso a um conjunto de recursos de forma eficiente e semelhante à arquitetura original do computador. Cada máquina virtual utiliza de forma individual e transparente os recursos existentes, sem a necessidade do conhecimento dos demais processos em execução.

Através da transparência no acesso aos recursos oferecida pela máquina virtual, os sistemas em execução sobre uma arquitetura virtualizada têm acesso ao *hardware* existente sem a necessidade da utilização de *software* específico. O monitor de máquinas virtuais oferece uma camada representando os recursos existentes através da qual posteriormente as interrupções serão interceptadas ou diretamente direcionadas para o *hardware* nativo, de acordo com a implementação do MMV.

Os monitores de máquinas virtuais podem ser implementados utilizando virtualização clássica ou virtualização hospedada [Smith and Nair 2005]. Na implementação utilizando virtualização clássica, o monitor de máquinas virtuais é executado diretamente sobre o *hardware* possuindo o nível mais alto de privilégio de execução de instruções. Neste modelo, todas as chamadas de sistema são interceptadas pelo MMV para posteriormente serem executadas. Já na implementação hospedada o monitor de máquinas virtuais executa sobre um sistema operacional existente, utilizando o nível mais baixo de privilégios. Neste modelo de implementação, o MMV utiliza tradução binária em tempo de execução para adaptar as instruções que necessitam de um maior nível de privilégios.

Os sistemas Xen [Barham et al. 2003] e VMware [Sugerman et al. 2001] utilizam respectivamente o modelo de implementação clássica e o modelo de implementação hospedada para oferecer a representação do *hardware* existente para os sistemas operacionais virtualizados.

2.1. Xen

O monitor de máquinas virtuais Xen [Barham et al. 2003] é uma ferramenta de código aberto desenvolvida pela Universidade de Cambridge, baseada na abordagem clássica de implementação de virtualização, onde o MMV possui o nível mais alto de privilégio.

A abordagem clássica de virtualização apresenta limitações em arquiteturas implementadas utilizando a especificação Intel IA-32, onde os sistemas operacionais virtualizados ainda conseguem executar instruções com um privilégio maior. Para contornar este problema arquitetural, o monitor Xen utiliza a técnica de **paravirtualização** para adaptar a execução dos sistemas operacionais virtualizados. Através da paravirtualização, Xen garante que os sistemas virtualizados não tenham acesso direto aos recursos disponíveis, permitindo desta forma uma virtualização eficiente sobre a arquitetura Intel x86.

A virtualização clássica implementada utilizando a técnica de paravirtualização requer pequenas alterações nos sistemas operacionais virtualizados, já que a interface oferecida pelo MMV difere em alguns pontos da interface real do computador. Efetuando-se estas alterações, um sistema operacional adaptado permite que os processos e serviços internos executem sem nenhuma alteração em seus códigos, sem impor uma sobrecarga limitante que comprometa o desempenho final das aplicações [Menon et al. 2005]. Atualmente, sistemas operacionais como Linux, NetBSD, FreeBSD, e Windows XP possuem implementações adaptadas para execução sobre a interface virtual implementada por Xen.

A implementação do monitor Xen é dividida especificamente entre o monitor de máquinas virtuais (*hypervisor*) e os domínios Xen, que são a representação das máquinas virtuais existentes. Nesta abordagem, as máquinas virtuais são gerenciadas através de chamadas realizadas para um domínio especial, denominado *Domain0*, através do qual é possível inicializar e terminar máquinas virtuais. Internamente, o monitor Xen utiliza os recursos do *Domain0* para ter acesso ao *hardware* e gerenciar a alocação de memória entre os demais domínios.

Além de gerenciar o acesso aos recursos de *hardware* existentes, o MMV Xen implementa através do *Domain0* um conjunto de chamadas de sistema que permitem migrar um sistema operacional entre computadores. A independência de *hardware* obtida pelo monitor Xen permite que máquinas virtuais sejam encapsuladas e migradas entre computadores com arquitetura virtualizada. Este processo de migração pode ser efetuado sem a interrupção dos serviços em execução sobre o sistema operacional virtualizado. O mecanismo de *live migration* [Clark et al. 2005] implementado por Xen utiliza técnicas que efetuam a migração completa de um sistema sem interromper a disponibilidade do serviço.

A migração de máquinas virtuais surge como ferramenta auxiliar para administradores de redes e servidores, já que um sistema operacional pode migrar sem interromper os serviços em execução, permitindo a manutenção do *hardware* do computador hospedeiro quando necessário. Porém, esta ferramenta somente pode ser utilizada em ambientes que utilizam um sistema de compartilhamento de arquivos e diretórios, já que a implementação atual do mecanismo de *live migration* não possui suporte para migração do sistema de arquivos local.

2.2. VMware

O monitor de máquinas virtuais VMware [Sugerman et al. 2001] é um produto desenvolvido pela empresa VMware Inc., utilizando a técnica de virtualização hospedada. Para tal, o sistema é dividido em VMApp, que é a máquina virtual que executa no espaço de usuário do sistema operacional hospedeiro e VMDriver, que é um *software* que executa junto ao sistema operacional hospedeiro e processa as requisições feitas pelo VMApp.

A máquina virtual provida por VMware apresenta ao sistema operacional hospedado um conjunto fixo de dispositivos, como interfaces de vídeo, áudio e rede, o que anula a necessidade de desenvolvimento de novos controladores por parte do sistema operacional hospedado. Sempre que o sistema hospedado faz uma um acesso a algum dispositivo virtual, o MMV salva o contexto da máquina virtual e muda para o seu contexto (*world switch*), onde é feito o acesso ao dispositivo real e retornando ao contexto da máquina virtual assim que a requisição estiver completa. Utilizando essa arquitetura, VMware pode ser utilizado para executar a maioria dos sistemas operacionais disponíveis no mercado, sem necessitar de alteração do código dos mesmos.

A memória das máquinas virtuais é gerenciada pelo monitor através da utilização de tabelas de página sombra (*shadow page tables*). Sempre que é feita uma leitura ou gravação na memória por parte de alguma máquina virtual, o MMV intercepta a instrução e acessa a localização real do dado.

A migração de uma máquina virtual para outro sistema hospedeiro é possível, porém com interrupção momentânea do sistema. Para tal, é feita uma cópia da memória utilizada pela máquina virtual para o novo hospedeiro, bem como o estado atual da máquina virtual e o arquivo com as configurações do BIOS (*Basic Input Output System*) virtual. O sistema de arquivos da máquina virtual precisa estar armazenado em algum sistema de armazenamento compartilhado, como por exemplo um sistema de armazenamento conectado à rede - NAS (*Network-Attached Storage*).

3. Virtualização de Recursos e o Gerenciamento de Redes

As vantagens obtidas pela utilização de um ambiente virtualizado têm sido exploradas em diversos trabalhos recentes nas áreas de redes e sistemas distribuídos.

Em ambientes distribuídos para a computação de alto desempenho, a virtualização surge como um mecanismo auxiliar na administração de *clusters* de computadores e grades computacionais [Huang et al. 2006, Figueiredo et al. 2003]. Em ambientes que necessitam de gerenciamento eficiente de redes e servidores, uma arquitetura virtualizada permite que diversas tecnologias sejam interligadas, auxiliando em diversas tarefas de administração dos recursos.

Servidores que utilizam virtualização oferecem vantagens em diversos aspectos como segurança e integridade dos processos em execução através da utilização de monitores de máquinas virtuais. Um exemplo de utilização de virtualização é encontrado nos servidores IBM Power5 [Stahl 2005], onde a virtualização é explorada para garantir independência e integridade dos serviços em execução através da transparência obtida com a utilização de máquinas virtuais.

Um servidor que utilize virtualização de recursos permite que cada máquina virtual hospede um serviço independente das demais, garantindo através do isolamento de

hardware que as falhas ocorridas em um serviço não se propaguem para os demais.

A intrusividade imposta pelo monitor de máquinas virtuais foi investigada em alguns trabalhos [Figueiredo et al. 2003, Childs et al. 2005]. Figueiredo et al. discutem a aplicabilidade de soluções de virtualização, analisando a sobrecarga imposta pelo MMV sobre as aplicações em execução (neste trabalho a virtualização foi implementada utilizando o monitor VMware). Já Childs et al. realizam um comparativo entre Xen e UML (*User Mode Linux*) [Dike 2006], buscando identificar a sobrecarga imposta sobre a utilização de um serviço específico composto por quatro servidores hospedados sobre uma mesmo computador. Em ambos os trabalhos, concluiu-se que a sobrecarga imposta pelos monitores de máquinas virtuais (considerando o melhor caso obtido nas investigações) é suficientemente tolerável considerando as vantagens obtidas através da virtualização dos recursos.

Recentemente, Quétier et al. apresentaram o resultado da execução de diversos *microbenchmarks* que investigaram a escalabilidade oferecida por quatro diferentes implementações de monitores de máquinas virtuais [Quétier et al. 2006]. Nesta avaliação, Xen destacou-se entre os demais monitores em diversos quesitos investigados, inclusive escalabilidade, sendo possível comprovar, através do conjunto de testes realizados, a possibilidade de utilização de virtualização em ambientes com recursos distribuídos. Este mesmo trabalho mostra que VMware, devido ao elevado número de trocas de contexto entre o sistema operacional hospedeiro e o hospedado (*world switch*), aliado à utilização de tabelas de página sombra para o gerenciamento da memória da máquina virtual, gera uma sobrecarga considerável sobre o sistema, o que pode comprometer a escalabilidade da solução.

Clark et al. investigaram a utilização do mecanismo de migração *live migration* implementado pelo MMV Xen [Clark et al. 2005], analisando tempos de migração e tempos de indisponibilidade de diferentes tipos de serviços virtualizados, como servidores Web e servidores de jogos (baixa latência). Os resultados obtidos neste trabalho concluem que a utilização de migração de máquinas virtuais em execução podem ser utilizadas como uma importante ferramenta na administração de redes e de servidores.

Por fim, há que se ressaltar o trabalho de McIlroy et al., que propõe a utilização de técnicas de virtualização na construção de roteadores com suporte à qualidade de serviço (QoS) [McIlroy and Sventek 2006]. Para tal, construiu-se um roteador que faz uso de Xen para gerenciar outros pequenos roteadores virtuais (*QoS routelets*), cada qual responsável por apenas um fluxo de dados. Dessa forma, o MMV pode garantir que cada *QoS routelet* pode acessar apenas a fatia de recursos físicos que compete à sua configuração, assim garantindo que um fluxo de dados não interfira no outro. Os autores chegam à conclusão de que a utilização de virtualização em roteadores pode ser factível, principalmente se a sobrecarga imposta pela utilização de tal solução puder ser diminuída.

4. Considerações Finais

Este trabalho discutiu a virtualização de recursos computacionais e seus benefícios para administradores de redes e servidores. Vantagens obtidas através dos monitores de máquinas virtuais, como migração de sistemas operacionais e independência de *hardware*, permitem que serviços em execução sejam migrados entre computadores interconectados, independente da tecnologia utilizada pelo hospedeiro.

Através da revisão bibliográfica realizada, percebe-se que a utilização de ambientes virtualizados é um assunto recorrente. Os resultados obtidos nas investigações concluem que a intrusividade imposta pelos monitores de máquinas virtuais em diversos contextos é suficientemente tolerável, considerando as vantagens obtidas através da virtualização dos recursos.

Referências

Barham, P., Dragovic, B., Fraser, K., Hand, S., Harris, T., Ho, A., Neugebauer, R., Pratt, I., and Warfield, A. (2003). Xen and the art of virtualization. In *Proceedings of the Nineteenth ACM symposium on Operating systems principles (SOSP)*, pages 164–177, Bolton Landing, NY, USA. ACM.

Childs, S., Coghlan, B., O'Callaghan, D., and and, G. Q. (2005). A single-computer grid gateway using virtual machines. In *Proc.19th International Conference on Advanced Information Networking and Applications (AINA'05)*.

Clark, C., Fraser, K., Hand, S., Hansen, J. G., Jul, E., Limpach, C., Pratt, I., and Warfield, A. (2005). Live migration of virtual machines. In *Proceedings of the Second Symposium on Networked Systems Design and Implementation (NSDI '05)*, Boston, MA, USA. Usenix.

Dike, J. (2006). *User Mode Linux*. Prentice Hall PTR.

Figueiredo, R., Dinda, P., and Fortes, J. (2003). A case for grid computing on virtual machines. In *Proc. International Conference on Distributed Computing Systems (ICDCS)*.

Goldberg, R. (1974). Survey of virtual machine research. *IEEE Computer*, 7(6):34–45.

Huang, W., Liu, J., Abali, B., and Panda, D. (2006). A case for high performance computing with virtual machines. *The 20th ACM International Conference on Supercomputing*.

McIlroy, R. and Sventek, J. (2006). Resource virtualisation of network routers. In *Workshop on High Performance Switching and Routing (HPSR 06)*.

Menon, A., Santos, J. R., Turner, Y., Janakiraman, G. J., and Zwaenepoel, W. (2005). Diagnosing performance overheads in the xen virtual machine environment. In *VEE '05: Proceedings of the 1st ACM/USENIX international conference on Virtual execution environments*, pages 13–23, New York, NY, USA. ACM Press.

Quétier, B., Neri, V., and Cappello, F. (2006). Scalability comparison of 4 host virtualization tools. Technical Report 1433, INRIA/LRI, Université Paris-Sud.

Smith, J. E. and Nair, R. (2005). The architecture of virtual machines. *IEEE Computer*, 38(5):32–38.

Stahl, E. (2005). Virtualization security and integrity in the IBM @server POWER5 environment. Technical Report 090105, IBM Systems and Technology Group.

Sugerman, J., Venkitachalam, G., and Lim, B.-H. (2001). Virtualizing I/O devices on VMware workstation's hosted virtual machine monitor. In *Proc. General Track: 2001 Usenix Annual Technical Conference*, pages 1–14. Usenix Assoc.