Uma ferramenta para gerência de rede de máquinas virtuais na emulação de ambientes distribuídos de larga escala

Mauro Strelow Storch, Prof. Dr. César A. F. De Rose

Pontifícia Universidade Católica do Rio Grande do Sul
Av. Ipiranga, 6681 - Porto Alegre/RS
{storch,derose}@inf.pucrs.br

Resumo

A virtualização de hardware pode ser explorada como ferramenta para o desenvolvimento de inúmeras aplicações. A emulação de ambientes distribuídos em larga escala é facilmente implementada através dos recursos que a virtualização oferece. Com pouco recurso computacional podemos simular um ambiente com centenas ou milhares de máquinas. A necessidade de uma ferramenta para gerenciar a rede deste ambiente surge como um ponto importante na criação de diferentes cenários distribuídos. A partir desses componentes, pode-se fazer execuções de software distribuídos em um ambiente controlado.

Motivação

Atualmente são feitos muitos estudos para integração da virtualização de hardware em diversas áreas de pesquisa. Muitos dos recursos oferecidos por essa tecnologia podem ser aplicados de diferentes formas e para diferentes finalidades [3].

A virtualização de hardware consiste em escalonar os recursos físicos entre vários software. Este princípio possibilita que através de virtualizadores do tipo Monitores de Máquinas Virtuais (VMM) possa-se executar mais de um Sistema Operacional em um mesmo computador [2]. A principal função do VMM é escalonar os recursos físicos como memória, CPU, disco e rede entre as Máquinas Virtuais (VM). Neste modelo de virtualização, as máquinas virtuais são cópias do hardware. Assim, a execução do sistema operacional em cada VM acontece de forma completamente independente.

É difícil a análise de aplicações distribuídas para *Clusters* e *Grids*. Com o auxilio da virtualização de hardware podemos simular diferentes tipos de ambientes através de máquinas virtuais, possibilitando a emulação de ambientes computacionais em larga escala. Com poucos recursos computacionais podemos simular, por exemplo, uma rede de computadores de centenas ou milhares de máquinas.

A simulação de aplicações distribuídas exige a comunicação de rede entre as máquinas [4]. Quando se simula um ambiente de larga escala em um ambiente com máquinas virtuais é necessária a configuração dos recursos para criar diferentes cenários de rede.

O Monitor de Máquinas Virtuais Xen [1] utiliza recursos de comunicação de rede comuns, baseados no sistema operacional Linux. Assim, podemos definir configurações de rede para conectar máquinas virtuais de um mesmo computador e com máquinas virtuais de outros computadores. Esse recurso nos permite criar domínios de rede com diferentes configurações permitindo a reprodução de ambientes de redes para, por exemplo, simulação e teste de aplicações distribuídas em *Clusters* e *Grids*.

Ferramenta

O Monitor de Máquinas Virtuais (VMM) *Xen* é uma camada de software que fica logo acima da camada de hardware. Ele é responsável por interceptar as instruções enviadas pelo sistema operacional e garantir a consistência e a segurança do sistema com um todo. Sobre ele encontram-se as Máquinas Virtuais que são cópias do hardware oferecido pelo VMM e suportam a execução de um sistema operacional. Classificamos essas VMs como privilegiadas e não-privilegiadas. Para cada computador temos uma VM privilegiada, que possui acesso ao hardware, e n não-privilegiadas, que possuem acesso restrito ao hardware.

O VMM oferece para cada VM uma cópia de todos os recursos físicos da máquina. O acesso à rede das VMs é feito através de um *switch* virtual. Nele encontram-se conectadas todas as interfaces virtuais de rede das VMs e também as interfaces de rede reais. Este *switch* é gerenciado por um *firewall* instalado na VM privilegiada.

Com base nestas definições foi feito um estudo de ferramentas *open source* para gerência de *firewalls*. As ferramentas estudadas oferecem amplo suporte para as questões de *firewall* e permitem que se possam emular diferentes configurações de rede. No entanto, tais ferramenta não tem o conhecimento das configurações de rede das VMs não-privilegiadas.

Este trabalho concentra-se na integração de uma ferramenta de gerência de *firewall* com as funcionalidades da virtualização de hardware. A partir dessa ferramenta é possível a gerência da rede de todo o ambiente criado pelas VMs, possibilitando que possam ser feitas alterações e reconfigurações do ambiente.

Referências

[1] P. Barham, B. Dragovic, K. Fraser, S. Hand, T. Harris, A. Ho, R. Neugebar, I. Pratt, and A. Warfield. Xen and the art of virtualization. In *Proceedings of the ACM Symposium on Operating Systems Principles (SOSP)*, October 2003.

[2] Christian Plessl and Marco Platzner. Virtualization of hardware - introduction and survey. In *ERSA*, pages 63–69, 2004.

[3] Mendel Rosenblum. The reincarnation of virtual machines. *ACM Queue*, 2(5):34–40, 2004.

[4] Andrew S. Tanenbaum. *Distributed Operating Systems*. Prentice Hall, 1995.