Virtualização: VMWare e Xen

Diogo Menezes Ferrazani Mattos
GTA/POLI/UFRJ
HTTP://www.gta.ufrj.br/

Abstract

Nowadays, the concept of virtualization is being remembered as a possible solution, which has low costs, to provide reliability, isolation and scalability to some systems. Some common uses of virtualization are the server's consolidation and the IT infra-structures virtualization. This paper discuss two types of virtualization: the full system virtualization, shown by the case study of VMWare, and the paravirtualization, shown by Xen.

Resumo

Atualmente o conceito de virtualização tem sido lembrado como uma possível solução de baixo custo para fornecer confiabilidade, isolamento e escalabilidade a alguns sistemas. Algumas utilizações cada vez mais comuns da virtualização são a consolidação de servidores e a virtualização da infra-estrutura de TI. Neste trabalho serão discutidos dois tipos de virtualização: a virtualização completa, representa pelo estudo de caso do VMWare, e a paravirtualização, representada pelo Xen.

1 – Introdução

A virtualização permite que em uma mesma máquina sejam executadas simultaneamente dois ou mais ambientes distintos e isolados. Esse conceito de virtualização remonta aos antigos mainframes, que deviam ser divididos por vários usuários em ambientes de aplicação completamente diferentes. Essa realidade da década de 1970 foi em grande parte superada nos anos de 1980 e 1990, com o surgimento dos computadores pessoais. No entanto, atualmente há uma onda crescente de interesse sobre as técnicas de virtualização.

Agora o interesse na virtualização não se atém somente ao fato de permitir o uso de um mesmo sistema por vários usuários concomitantemente, mas os principais interesses são a segurança, confiabilidade e disponibilidade, custo, adaptabilidade, balanceamento de carga e suporte a aplicações legadas.

1.1 – Histórico

Os primeiros computadores que surgiram eram gigantescos e muito caros. No entanto, devido à grande demanda por uso, estes rapidamente se tornaram indispensáveis. Para socializar o uso dos computadores foi criado, no final dos anos 1960, o *time-sharing*, que permitia o uso de um mesmo computador por vários usuários simultaneamente de forma transparente. Embora este tenha

sido um grande passo na história da computação, surgia assim um novo problema, o compartilhamento de um único computador com outras aplicações suscetíveis a falhas.

A fim de sanar esse problema, a primeira solução proposta foi o uso de vários computadores, o que se reverteria em um aumento significativo do desempenho e na garantia de isolamento entre as aplicações. Entretanto esta solução apresentava um altíssimo custo, além de ser um desperdício de recursos, já que os computadores ficavam grande parte do tempo ociosos. Tendo isto em vista, nos anos 60 a IBM começou a desenvolver a primeira máquina virtual, que permitia que um único computador fosse dividido em vários.

O primeiro sistema de virtualização desenvolvido foi o CP-67, *software* para o mainframe IBM 360/67, que disponibilizava ao usuário um sistema virtual do /360 da IBM. Os resultados obtidos com esse sistema foram ótimos.

Após o CP-67, a IBM lançou o VM/370, um VMM (*Virtual Machine Monitor*, ou Monitor de Máquina Virtual) para o Sistema /370 com arquitetura estendida, ou seja, com algumas instruções extras que permitiam a virtualização. Essas foram as primeiras tentativas de virtualização.

Em um cenário mais atual, a arquitetura mais comum é a x86 (IA-32). Essa é a arquitetura adotada pelos PCs, que se tornaram *commodities*. Ao contrário da arquitetura dos antigos sistemas /370 com arquitetura estendida, que apresentavam instruções que visavam a virtualização, a arquitetura x86 não foi projetada considerando a virtualização. Isso pode ser visto em pequeno conjunto de instruções que não necessitam de um modo privilegiado para serem executadas, mas podem prejudicar a estabilidade do sistema.

Ainda que seja difícil desenvolver um VMM para a arquitetura x86, algumas técnicas podem ser usadas para romper com as dificuldades impostas pelo conjunto de instruções desta arquitetura. Voltados para a arquitetura x86, podem ser citados alguns projetos relacionados, tais como VMWare, Xen, Virtual PC, Citrix, Hyper-V, entre outros.

1.2 – Definições e Conceitos

Os primeiros conceitos que devemos ter em relação à virtualização são de instruções privilegiadas e não privilegiadas. Essas instruções fazem parte do conjunto de instruções da arquitetura em questão, neste trabalho a arquitetura considerada é x86. As instruções não-privilegiadas são aquelas que não modificam a alocação ou o estado de recursos compartilhados por vários processos simultâneos, tais como processadores, memória principal e registradores especiais. Em oposição a essas instruções, temos as instruções privilegiadas, que podem alterar o estado e a alocação desses recursos.

Um computador pode operar em dois modos distintos, o modo de usuário ou o de supervisor. O modo de usuário, também chamado de espaço de aplicação, é modo no qual as aplicações normalmente são executadas. Neste modo, não é possível executar as instruções privilegiadas, que são restritas ao modo de supervisor.

O modo de supervisor tem o controle total sobre a CPU, podendo executar todas as instruções do conjunto de instruções do processador em questão, tanto as não-privilegiadas como as privilegiadas. O sistema operacional é executado neste modo. Antes de o sistema operacional passar o controle da CPU para uma aplicação do usuário, o *bit* de controle de modo é configurado para o modo de usuário.

Vale lembrar que na arquitetura em questão, x86, existem quatro níveis de privilégio, que são chamados de *rings*. Os *rings* são numerados de 0 a 3, nos quais o nível 0 é o que tem maior

privilégio na execução de instruções, por isso, os sistemas operacionais são executados com esse nível de privilégio.

Já em um ambiente virtualizado, temos que definir mais dois conceitos, os de sistema operacional hospedeiro e o de sistema operacional visitante. O primeiro, sistema operacional hospedeiro (*Host Operating System*), refere-se ao sistema operacional nativo da máquina na qual ocorrerá a virtualização, ou seja, este é o sistema operacional que é executado diretamente sobre o *hardware* físico. O segundo, sistema operacional visitante (*Gest Operating System*), refere-se ao sistema operacional que é executado sobre o *hardware* virtualizado, isto é, o sistema operacional que é executado na máquina virtual. Uma máquina na qual é feita a virtualização pode contar com apenas um SO hospedeiro sendo executado por vez. No entanto, podem ser executados diversos SOs visitantes simultaneamente.

O próximo conceito a ser discutido é de vital importância para o entendimento da virtualização. O conceito em questão é o do *Virtual Machine Monitor* (VMM), ou seja, Monitor de Máquina Virtual, também conhecido por *Hypervisor*.

O *Virtual Machine Monitor* é um componente de *software* que hospeda as máquinas virtuais [6]. O VMM é responsável pela virtualização e controle dos recursos compartilhados pelas máquinas virtuais, tais como, processadores, dispositivos de entrada e saída, memória, armazenagem. Também é função do VMM escalonar qual máquina virtual vai executar a cada momento, semelhante ao escalonador de processos do Sistema Operacional [5].

O VMM é executado no modo de supervisor, no entanto as máquinas virtuais são executadas em modo de usuário. Como as máquinas virtuais são executadas em modo de usuário, quando estas tentam executar uma instrução privilegiada, é gerada uma interrupção e o VMM se encarrega de emular a execução desta instrução.

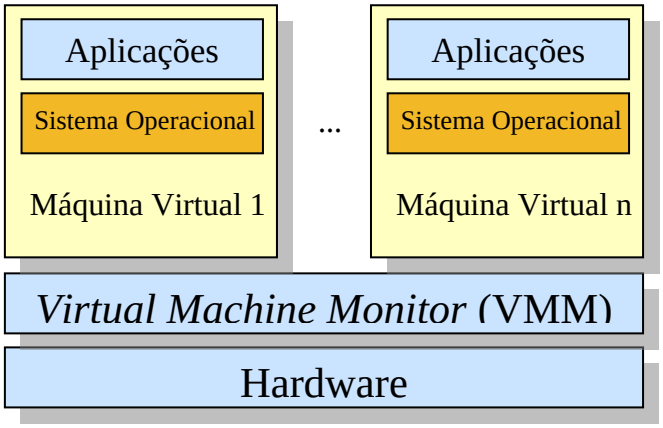

Figura 1: Relacionamento das Máquinas Virtuais e do VMM [6].

2. Vantagens e Desvantagens

Existem diversas vantagens na virtualização, a seguir serão citadas as principais [5]:

a) Segurança: Usando máquinas virtuais, pode ser definido qual é o melhor ambiente para executar cada serviço, com diferentes requerimentos de segurança, ferramentas diferentes e o sistema operacional mais adequado para cada serviço. Além disso, cada máquina virtual é isolada das demais. Usando uma máquina virtual para cada serviço, a vulnerabilidade de um serviço não prejudica os demais.

b) Confiança e disponibilidade: A falha de um *software* não prejudica os demais serviços.

c) *Custo*: A redução de custos é possível de ser alcançada com a consolidação de pequenos servidores em outros mais poderosos. Essa redução pode variar de 29% a 64% [5].
d) *Adaptação às diferentes cargas de trabalho*: Variações na carga de trabalho podem ser tratadas facilmente. Ferramentas autônomas podem realocar recursos de uma máquina virtual para a outra.
e) *Balanceamento de carga:* Toda a máquina virtual está encapsulada no VMM. Sendo assim é fácil trocar a máquina virtual de plataforma, a fim de aumentar o seu desempenho.
f) *Suporte a aplicações legadas*: Quando uma empresa decide migrar para um novo Sistema Operacional, é possível manter o sistema operacional antigo sendo executado em uma máquina virtual, o que reduz os custos com a migração. Vale ainda lembrar que a virtualização pode ser útil para aplicações que são executadas em *hardware* legado, que está sujeito a falhas e tem altos custos de manutenção. Com a virtualização desse *hardware*, é possível executar essas aplicações em *hardwares* mais novos, com custo de manutenção mais baixo e maior confiabilidade.

Por outro lado, existem as desvantagens da virtualização, sendo as principais:

a) *Segurança*: Segundo Neil MacDonald, especialista de segurança da Gartner, hoje em dia, as máquinas virtuais são menos seguras que as máquinas físicas justamente por causa do VMM [2]. Este ponto é interessante, pois se o sistema operacional hospedeiro tiver alguma vulnerabilidade, todas as máquinas virtuais que estão hospedadas nessa máquina física estão vulneráveis, já que o VMM é uma camada de *software*, portanto, como qualquer *software*, está sujeito a vulnerabilidades.
b) *Gerenciamento*: Os ambientes virtuais necessitam ser instanciados, monitorados, configurados e salvos [2]. Existem produtos que fornecem essas soluções, mas esse é o campo no qual estão os maiores investimentos na área de virtualização, justamente por se tratar de um dos maiores contra-tempos na implementação da virtualização. Vale lembrar que o VMWare é a plataforma mais flexível e fácil de usar, mas ainda apresenta falhas que comprometem a segurança, assim como as demais plataformas [2].
c) *Desempenho*: Atualmente, não existem métodos consolidados para medir o desempenho de ambientes virtualizados. No entanto, a introdução de uma camada extra de *software* entre o sistema operacional e o *hardware*, o VMM ou *hypervisor*, gera um custo de processamento superior ao que se teria sem a virtualização. Outro ponto importante de ressaltar é que não se sabe exatamente quantas máquinas virtuais podem ser executadas por processador, sem que haja o prejuízo da qualidade de serviço.

3. Virtualização total e para-virtualização

Existem duas formas de implementação dos monitores de máquina virtual: a virtualização total e a para-virtualização.

A virtualização total tem por objetivo fornecer ao sistema operacional visitante uma réplica do *hardware* subjacente. Dessa forma, o sistema operacional visitante é executado sem modificações sobre o monitor de máquina virtual (VMM), o que traz alguns inconvenientes. O primeiro é que o número de dispositivos a serem suportados pelo VMM é extremamente elevado. Para resolver esse contratempo, as implementações da virtualização total usam dispositivos genéricos, que funcionam bem para a maioria dos dispositivos disponíveis, mas não garantem o uso

da totalidade de sua capacidade. Outro inconveniente da virtualização total é o fato de o sistema operacional visitante não ter conhecimento de que está sendo executado sobre o VMM, então as instruções executadas pelo sistema operacional visitante devem ser testadas pelo VMM para que depois sejam executadas diretamente no *hardware*, ou executadas pelo VMM e simulada a execução para o sistema visitante. Por fim, o último inconveniente da virtualização total é o fato de ter que contornar alguns problemas gerados pela implementação dos sistemas operacionais, já que esses foram implementados para serem executados como instância única nas máquinas física, não disputando recursos com outros sistemas operacionais. Um exemplo desse último inconveniente é uso de paginação na memória virtual, pois há a disputa de recursos entre diversas instâncias de sistemas operacionais, o que acarreta em uma queda do desempenho [2].

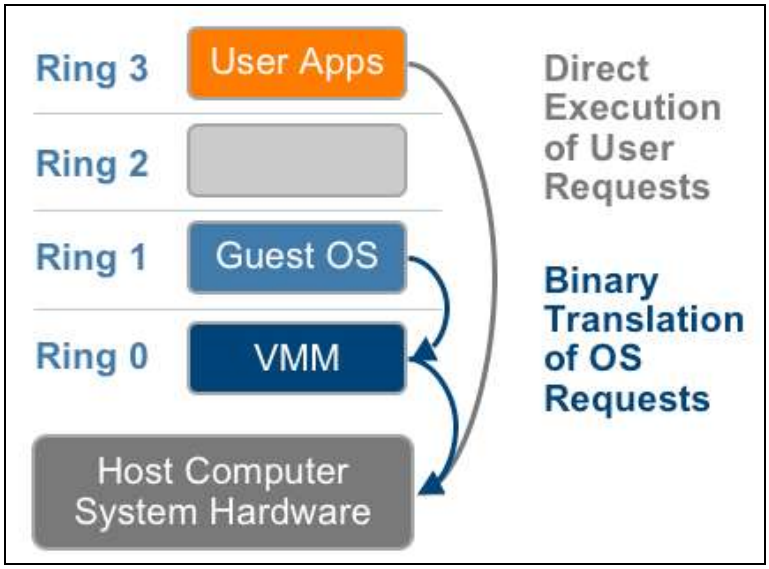

Figura 2: Virtualização total na arquitetura x86 [11].

A para-virtualização é uma alternativa à virtualização total. Nesse modelo de virtualização, o sistema operacional é modificado para chamar o VMM sempre que executar uma instrução que possa alterar o estado do sistema, uma instrução sensível. Isso acaba com a necessidade de o VMM testar instrução por instrução, o que representa um ganho significativo de desempenho. Outro ponto positivo da para-virtualização é que os dispositivos de *hardware* são acessados por *drivers* da própria máquina virtual, não necessitando mais do uso de *drivers* genéricos que inibiam o uso da capacidade total do dispositivo.

Embora a para-virtualização apresentasse um ganho de desempenho significativo frente à virtualização total, essa disparidade tem sido superada devido à presença de instruções de virtualização nos processadores Intel e AMD, que favorecem a virtualização total. A tecnologia de virtualização da Intel é a IVT (*Intel Virtualization Technology*), codinome *Vanderpool*. A da AMD é a AMD-V (*AMD-Virtualization*), codinome *Pacífica*. Embora tenham sido desenvolvidas para o mesmo propósito, foram desenvolvidas de maneira independentes. Por esse motivo, há alguns problemas na portabilidade de máquinas virtuais de uma arquitetura Intel para a arquitetura AMD e vice-versa.

Portanto, tendo em vista as técnicas de virtualização, a decisão de qual melhor a técnica de virtualização para um dado ambiente está intimamente ligada a qual o processador da máquina física que vai hospedar as virtuais, bem como se o processador possui ou não uma extensão no seu conjunto de instruções que suporte a virtualização.

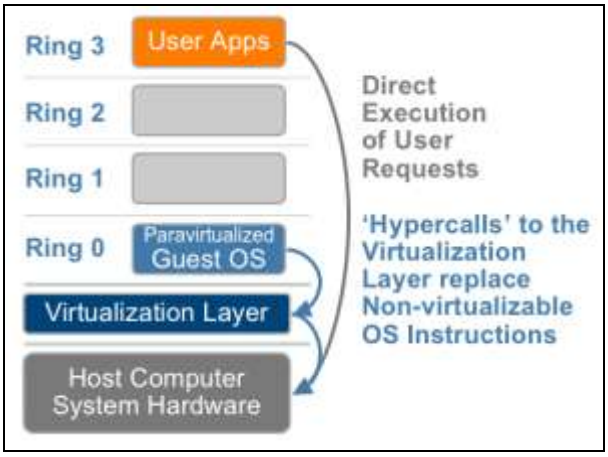

Figura 3: Para-virtualização na arquitetura x86.

3. Ferramentas de virtualização

Nesta seção serão abordadas as duas principais ferramenta de virtualização para a arquitetura x86: o VMWare e o Xen. Ambos são produtos de mercado, porém possuem algumas diferenças na implementação das técnicas de virtualização. A primeira e mais marcante é o fato de que o VMWare é um exemplo de virtualização total, enquanto o Xen é de para-virtualização.

3.1 – VMWare

O VMWare é um dos mais populares arcabouços de virtualização para a arquitetura x86. O VMWare é uma infra-estrutura de virtualização, fornecendo *softwares* para virtualização desde ambientes *desktop* a ambientes de *data centers*. Os produtos disponibilizados dividem-se em três categorias: gerenciamento e automação, intra-estrutura virtual e plataformas de virtualização [9]. O VMWare é executado como se fosse um programa, no espaço de aplicação, dentro de um sistema operacional hospedeiro, o qual fica responsável pela abstração dos dispositivos que serão disponibilizados para o sistema operacional visitante. Para ter acesso mais rápido aos dispositivos, o VMWare instala um *driver* especial que permite contornar o problema de ter que suportar um amplo conjunto de dispositivos para a arquitetura x86.

Entre os produtos fornecidos pela VMWare, podemos encontrar o VMWare Workstation, Server, Fusion e Player, que são plataformas de virtualização que são executadas em um sistema operacional hospedeiro. No entanto, há outra plataforma, VMWare ESX, que é, por si mesma, um sistema operacional hospedeiro. Este apresenta desempenho melhor que os demais, mas reduz a portabilidade [7].

Na arquitetura do VMWare, a virtualização ocorre a nível de processador. As instruções privilegiadas a serem executadas são capturadas e virtualizadas pelo VMM, enquanto que as outras instruções são executadas diretamente no processador hospedeiro [7].

Os recursos de *hardware* também são virtualizados. O suporte para os diversos dispositivos é fornecido pelo próprio sistema operacional hospedeiro. Para ter acesso aos dispositivos, o VMWare instala um *driver* de dispositivo, o *VMDriver*. Este *driver* põe a placa de rede em modo promíscuo, recebendo todos os quadros ethernet, e cria uma ponte (*bridge*), que encaminha os quadros para o sistema hóspede ou para a máquina virtual especificada.

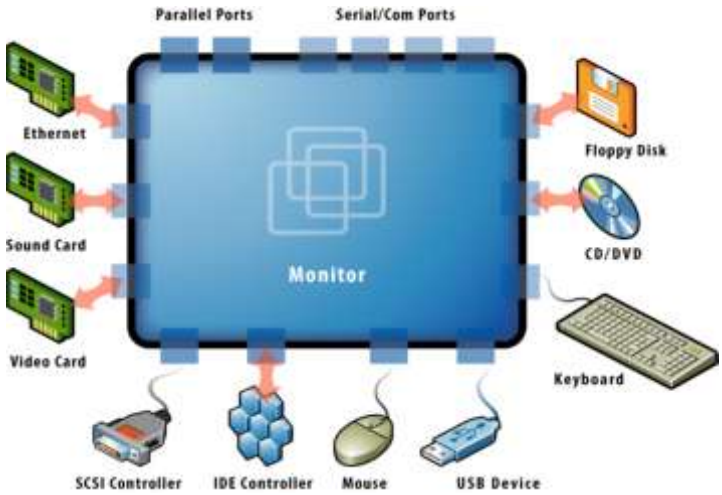

Figura 4: Virtualização dos dispositivos no VMWare [11].

3.2 – Xen

O Xen é um dos mais populares exemplos de para-virtualização. Na virtualização total, o sistema operacional visitante tenta executar tarefas protegidas e, por estarem no espaço de aplicação do sistema operacional hospedeiro, não podem ser executadas. No entanto, o VMM intervem e executa ou simula a execução dessas, o que reduz o desepenho da virtualização total. Já a para-virtualização apresenta-se como uma alternativa a isso, na medida em que o sistema operacional visitante é modificado para não tentar executar diretamente na CPU as tarefas protegidas, mas entregar essas ao VMM. Este tipo de virtualização tem um ganho de desempenho significativo frente à total.

Uma das maiores vantagens do uso do Xen como VMM na para-virtualização é o fato de que este apresenta um desempenho melhor do que os produtos de virtualização total, quando a máquina física hospedeira não tem instruções de *hardware* de suporte a virtualização. No entanto, há a necessidade de que o sistema visitante seja portado para o Xen, o que não chega a ser uma desvantagem, já que os sistemas operacionais mais comuns no mercado têm versões para o Xen. Alguns dos sistemas suportados pelo Xen são Linux, FreeBSD e Windows XP.

A tecnologia de virtualização provida pelo Xen difere da tecnologia do VMWare. O Xen segue o conceito da para-virtualização, que fornece um conjunto de abstrações (processador virtual, memória virtual, rede virtual etc.) sobre o qual diferentes sistemas podem ser portados [7]. As abstrações não são necessariamente similares ao *hardware* da máquina física hospedeira.

Para entender como o Xen implementa a para-virtualização, é importante salientar dois conceitos: o de domínio e o de *hypervisor*. Os domínios são as máquinas virtuais do Xen. Essas podem ser de dois tipos, privilegiadas (domínio 0) e não-privilegiadas (domínio U). O *hypervisor* é o responsável por controlar os recursos de comunicação, de memória e de processamento das máquinas virtuais, mas não possui os *drivers* para manipular os dispositivos diretamente.

Quando a máquina hospedeira é iniciada, uma máquina virtual do domínio 0, privilegiado, é criada. Esse domínio acessa uma interface de controle e executa aplicações de gerenciamento. As máquinas virtuais dos domínios U só podem ser criadas, iniciadas e desligadas através do domínio 0. Na máquina virtual do domínio 0, é executado um Linux com núcleo modificado, que pode acessar os recursos da máquina física, já que possui privilégios especiais, e ainda se comunicar com as outras máquinas virtuais, domínio U.

O sistema operacional do domínio 0 tem que ser modificado para possuir os *drivers* de dispositivo da máquina física e dois *drivers* que tratam requisições de acessos à rede e ao disco

realizadas pelas máquinas virtuais do domínio U. Em suma, só a máquina virtual do domínio 0 tem acesso direto aos recursos da máquina física, enquanto que as demais máquinas virtuais têm acesso a uma abstração dos recursos, que para serem acessados, as máquina virtuais dos domínios U têm que acessar através do domínio 0.

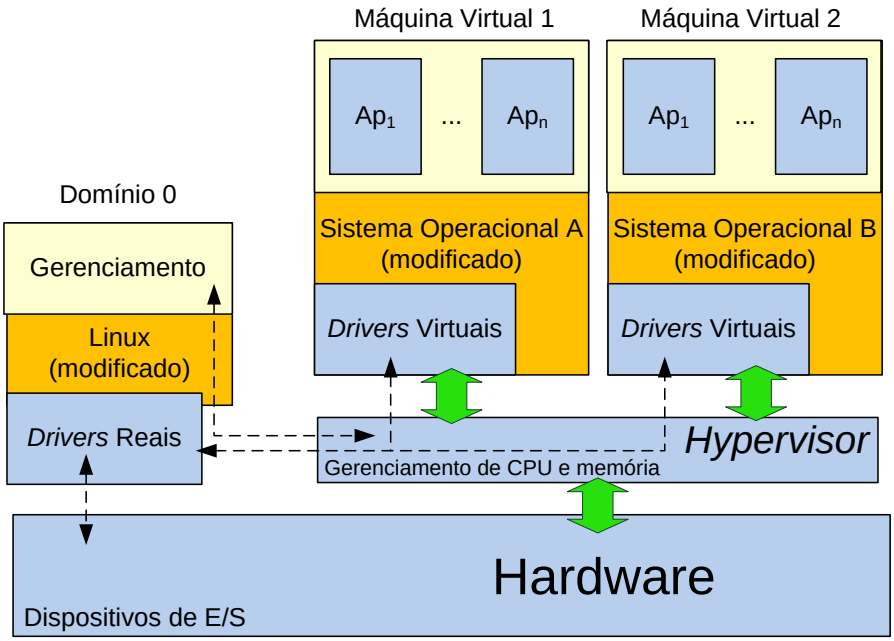

Figura 5: Componentes do Xen: *hypervisor* e domínios [2].

Para a virtualização da memória, o Xen reserva para cada máquina virtual uma determinada quantidade de memória, que pode ser alterada a qualquer momento sem a necessidade de terminar ou reiniciar a máquina virtual. Cada máquina virtual pode ter uma ou mais interfaces de rede virtuais. A comunicação entre as interfaces é implementada por dois *token rings*, um para enviar e outro para receber [7].

Atualmente, o Xen conta também com um domínio no qual é feita a virtualização total, o que permite que sistemas operacionais não modificados sejam executados sobre o *hypervisor* Xen. Inicialmente, a escolha pela para-virtualização justificava-se pelo fato de que o ganho em desempenho era muito maior do que com a virtualização total. No entanto, com o advento das arquiteturas AMD-V e Intel VT, arquitetura que dão o suporte de *hardware* para a virtualização, a virtualização total passou a obter resultados de desempenho melhores que os da para-virtualização. Vale ressaltar que o domínio de virtualização total disponível no Xen a partir da sua versão 3.0, só pode ser usado nas máquinas hospedeiras que possuam suporte de *hardware* à virtualização.

5. Comparação

A introdução do VMM entre o sistema operacional visitante e o *hardware* introduz um custo a mais no desempenho da máquina. No entanto, dependendo da configuração da máquina, da aplicação que está sendo executada e alguns outros fatores, esse custo pode ser maior com o uso da virtualização total ou da para-virtualização. A seguir será mostrado um quadro comparativo, com os estudos publicados em [9] e [11], pela VMWare e XenSource, respectivamente. Nos estudos da VMWare foram usados o VMWare Server ESX 3.01 e o XenEnterprise 3.03, já nos estudos da XenSource, foram usados o VMWare Server ESX 3.01 e o XenEnterprise 3.2.

Atualmente não existem testes de desempenho (*benchmarks*) especializados para máquinas virtuais. Sendo assim, nesses estudos foram realizados testes comuns para a medida de desempenho de computadores. Os testes foram: SPECcpu2000 Integer, compara basicamente computação a nível de usuário, focado em aplicações de computação intensiva; Passmark, gera uma carga de trabalho para testar os principais subsistemas que compõem um sistema operacional; NetPerf, avalia o desempenho da rede; SPECjbb2005, representa um servidor e sua carga; e a compilação do pacote SPECcpu2000 INT.

Teste	Resultados da VMWare	Resultados da XenSource
SPECcpu2000 Integer	O VMWare ESX mostrou uma perda de desempenho de 0-6%, enquanto o XenEnterprise 3.03 teve um desempenho de 1-12% menor do que a máquina nativa.	O desempenho dos dois foi praticamente igual. Enquanto o Xen mostrou um desempenho 3% menor que a máquina nativa, o VMWare mostrou uma queda de 2%.
Passmark	Comparado ao sistema nativo, o VMWare mostrou uma queda de desempenho de 4-18% e o Xen, 6-41%	Ambos obtiveram desempenho semelhante. No entanto, em um dos testes o VMWare obteve uma vantagem de 3,5% sobre o Xen.
NetPerf	Compartivamente, o VMWare obteve um resultado muito próximo ao do sistema nativo, a cima de 95%. Enquanto o Xen 3.03 não chegou a 5% do desempenho do sistema nativo.	O Xen 3.2 e o VMWare ESX 3.01 obtiveram resultados equivalentes.
SPECjbb2005	O ESX Server obteve resultados próximo a 90% do desempenho do sistema nativo, já o Xen não foi testado pois a versão 3.03, não tem suporte a configuração SMP virtual.	Desempenho semelhante do ESX e do Xen 3.2. Para dois processadores virtuais, o Xen supera o VMWare com 1,5% de vantagem, já para quatro processadores virtuais, o VMWare supera o Xen com 1% de vantagem.
SPECcpu2000 INT	O VMWare ESX 3.01 obteve um resultado equivalente a 90% do resultado do sistema nativo, enquanto o Xen 3.03 obteve somente 68% do sistema nativo.	Desempenhos próximos. O VMWare tem um desempenho pouco superior ao Xen, em torno de 6%.

Tabela 1: Comparação entre o VMWare ESX Server e o XenEnterprise

Tendo em vista os dados da comparação e levando em consideração que as configurações das máquinas usadas para os testes da VMWare e da XenSource não apresentam a mesma configuração, mas ambas dão suporte de *hardware* para a virtualização, é possível perceber que a virtualização total, representada pelo VMWare ESX Server 3.01, obteve os melhores resultados nos dois testes. No entanto, nos testes realizados pela XenSource, o Xen apresenta alguns aspectos melhores que o VMWare, mas não são resultados significativos.

Vale ressaltar ainda que o desempenho do sistema virtualizado está muito próximo do sistema nativo, o que sugere que a sobre-carga imposta pelo VMM não é tão significante, considerando uma máquina com suporte de *hardware* para a virtualização.

6. Uso da virtualização

6.1. Consolidação de Servidores

Um pensamento comum entre administradores de rede é de ter um servidor por serviço. Esta medida garante uma maior segurança e maior disponibilidade dos serviços na rede, já que a falha de um servidor só afeta um serviço e a vulnerabilidade de um serviço só expõe um servidor. No entanto, a taxa de utilização dos recursos de *hardware* de um servidor é extremamente baixa, o que indica uma subutilização de seus recursos.

A consolidação de servidores consiste em usar uma máquina física com diversas máquinas virtuais, sendo uma para cada servidor. Essa nova abordagem garante o isolamento dos servidores e apresenta as vantagens de aumentar a taxa de utilização de servidores, reduzir os custos operacionais, criar ambientes mais flexíveis e reduzir custos de administração de TI. O ponto mais importante da consolidação de servidores é o melhor aproveitamento dos recursos, já que se existem n servidores com uma taxa de utilização x, tal que $x < 100\%$, é menos custoso e mais vantajoso consolidar os n servidores em apenas um, com taxa de utilização de $n.x$, desde que $n.x < 100\%$.

Outro ponto a ser levantado é que a consolidação permite ocupar menos espaço físico com servidores, pois estes passam a ser apenas uma máquina física. Isso propicia menos gastos com eletricidade, já que o número de máquinas é menor, e com manutenção de máquinas. Vale ainda lembrar que a virtualização aumenta a flexibilidade, pois pode-se instalar diversos ambientes em uma mesma máquina, por exemplo, ter serviços que são executados em ambiente Windows, coexistindo em uma mesma máquina física, mas em máquinas virtuais distintas, que serviços que são executados em ambiente Linux.

6.2. Virtualização da Infra-estrutura de TI

A virtualização da infra-estrutura de TI diferencia-se da consolidação de servidores na medida em que a consolidação só prevê o isolamento dos servidores em máquinas virtuais, enquanto a virtualização da infra-estrutura de TI vai mais além. A virtualização da infra-estrutura de TI prevê a virtualização de toda a estrutura da rede, com a criação de comutadores, roteadores e outros equipamentos virtuais, interconectado às máquinas virtuais. Outro ponto de distinção entre a consolidação e a virtualização da infra-estrutura é que esta permite a alocação dinâmica de recursos para as máquinas virtuais, levando a um processo de automação da infra-estrutura de TI.

6.3. Laboratórios de ensino

A aplicação da virtualização em laboratórios de ensino tem por objetivo criar um ambiente que isole o estudante da máquina física. O estudante tem acesso a uma instância de uma máquina virtual, que pode ser facilmente recuperada de uma falha após o seu uso. Também é interessante notar que em ambientes virtualizados, a introdução de mais um sistema operacional no laboratório, não envolve a reinstalação das máquinas, mas somente a cópia dos arquivos de configuração e controle da máquina virtual do novo sistema operacional para as máquinas hospedeiras.

Em suma, a virtualização de laboratórios de ensino tem como vantagens a redução dos custos de manutenção, aumento da flexibilidade e aumento da segurança.

6.4. Desenvolvimento de Software

Em um ambiente de desenvolvimento de *software*, o uso de ambientes virtuais tem dois objetivos principais. O primeiro é fornecer ambientes distintos, com sistemas operacionais diferentes ou de diferentes versões, para que se possa testar o *software* e verificar o seu comportamento em outros ambientes, concomitantemente. O segundo é criar ambientes isolados no qual uma falha do *software* que está sendo desenvolvido não comprometa o sistema operacional da máquina hospedeira. Se o *software* em desenvolvimento vier a comprometer o sistema da máquina virtual, este pode ser recuperado copiando os arquivos de outra máquina, ou recuperando os arquivos da máquina comprometida do último *backup*.

7. Conclusão

A virtualização é uma técnica que está cada vez mais presente na área de TI. Isso vem sendo revelado pelo grande número de empresas que surgem com soluções de gerência de ambientes virtualizados e pelo aumento sucessivo nos investimento na área [2]. Essa técnica não é recente, mas após a popularização do PC, ela perdeu um pouco de destaque no cenário da TI. No entanto, esse destaque que vem sendo dado à virtualização recentemente é fruto do aumento do poder computacional, que não foi seguido pela taxa de utilização dos computadores, o que gerou muitos recursos ociosos. A fim de aproveitar esses recursos, a idéia da virtualização retornou ao cenário da TI.

Embora a técnica da virtualização pareça ser a solução para grande parte dos problemas de infra-estrutura de TI, sua aplicação deve ser estudada e devem ser avaliados os transtornos que podem ser gerados. A aplicação da técnica da virtualização traz consigo uma mudança de paradigma e, portanto, deve ser avaliada como um projeto de longo prazo. A sua adoção implicará na mudança de política de compras e instalação de novos sistemas.

Outro ponto a ser destacado na adoção da técnica de virtualização é qual vertente deve ser seguida, a virtualização total ou a para-virtualização. Cada uma tem sua especificidade e a escolha de qual é melhor para o ambiente de trabalho está intimamente ligada a qual será o *hardware* subjacente às máquinas virtuais. Caso seja um *hardware* com suporte à virtualização, ou seja, da arquitetura AMD-V ou Intel VT, o mais aconselhável é o uso do virtualização total. Caso contrário, o aconselhável é o uso da para-virtualização, que obteve melhores resultados de desempenho em teste realizados com *hardware* sem suporte à virtualização [7].

Em suma, a proposta da virtualização é muito atraente e traz diversos benefícios. Entretanto, como todo sistema computacional, está sujeito a falhas. A adoção da virtualização como paradigma a ser seguido é uma decisão que deve ser tomada avaliando uma série de fatores e ponderando os riscos e os benefícios. Portanto, para empregar a técnica de virtualização, o mais correto a ser feito é um projeto de longo prazo, que adote a virtualização em pequenos passos.

Para finalizar, vale lembrar que esta é uma área que está em crescimento e que novos produtos surgem a todo o momento. Portanto, existem questões que ainda não estão completamente resolvidas, tais como a migração de máquinas, a configuração automática de máquinas virtuais, facilidades de *backup* e a recuperação de falhas [2].

8. Perguntas e Respostas

8.1. A virtualização não é um conceito novo. Por que ficou esquecido durante tanto tempo?

O conceito de virtualização ficou esquecido, pois o objetivo principal da virtualização, quando esta foi criada, década de 60, era fornecer ambientes distintos dentro de um mainframe que

permitisse executar uma aplicação legada de outro mainframe. Essa necessidade de vários ambientes para aplicações legadas foi sendo perdida com o passar do tempo e o advento do microcomputador. Com o microcomputador, a arquitetura e os sistemas operacionais convergiram para uma unificação de padrões.

Atualmente, a virtualização tem voltado ao cenário das discussões. Isso ocorre, pois o poder computacional tem crescido em uma velocidade mais rápida do que a necessidade de processamento de dados, o que gera um poder computacional ocioso muito elevado. A virtualização desponta como uma proposta de melhor aproveitar o poder computacional ocioso e, assim, cortar custos operacionais e de administração em TI.

8.2. O que é o hypervisor ou VMM (Virtual Machine Monitor – Monitor de Máquina Virtual)?

O *hypervisor*, ou Monitor de Máquina Virtual (VMM), é uma camada de *software* entre o *hardware* e o sistema operacional. O VMM é responsável por fornecer ao sistema operacional visitante a abstração da máquina virtual. É o *hypervisor* que controla o acesso dos sistemas operacionais visitantes aos dispositivos de *hardware*. É interessante ressaltar que o VMM não executa em modo usuário, pois é ele que deve executar, ou simular a execução, das instruções privilegiadas requisitadas pelo sistema operacional visitante.

8.3. Qual a diferença prática entre para-virtualização e virtualização total?

A principal diferença prática entre a para-virtualização e a virtualização total é que na primeira o sistema operacional visitante tem que ser modificado para ser executado sobre o VMM, enquanto na segunda o VMM fornece uma réplica da máquina física, de modo que não tem a necessidade de que o sistema operacional visitante seja modificado para ter ciência de que está sendo executado em uma máquina virtual. Outra diferença a ser notada entre as duas técnicas de virtualização é o fato de que, na virtualização total, o sistema operacional visitante tem acesso direto aos dispositivos de *hardware*, enquanto na para-virtualização só o sistema operacional do domínio 0 tem acesso direto aos dispositivos e as demais máquinas virtuais dos domínios U só acessam os dispositivos através do domínio 0.

8.4. Na para-virtualização, qual é a diferença entre domínio 0 e domínio U?

O domínio 0 é uma máquina virtual especial que tem acesso direto aos dispositivos. Essa máquina virtual executa um núcleo Linux modificado, que é iniciado antes de qualquer outra máquina virtual. As demais máquinas virtuais são pertencentes ao domínio U. Essas máquinas só podem ser criadas, iniciadas e terminadas através do domínio 0. O *hypervisor*, na para-virtualização, não é capaz de fazer a comunicação entre sistema hospedeiro e sistema convidado. Portanto, há a necessidade da máquina virtual no domínio 0, para que haja a comunicação entre as demais máquinas e os dispositivos de *hardware*, já que só a máquina do domínio 0 acessa os dispositivos.

8.5. A consolidação de servidores é um processo seguro?

A consolidação de servidores tem como um de seus objetivos aumentar a segurança. No entanto, quando tratamos de virtualização há mais uma camada de *software* que deve ser inserida entre o *hardware* e o sistema operacional visitante: o Monitor de Máquina Virtual, VMM. Como todo *software*, o VMM está sujeito a falhas e a vulnerabilidades. Sendo assim, a segurança do processo de consolidação de servidores é abalada pela inclusão do VMM. Contudo, usando

softwares atualizados e mantendo sempre o uma cópia de segurança dos servidores virtuais, o procedimento de consolidação pode ser tão seguro quanto o uso de uma máquina física para cada servidor, pois a virtualização garante o isolamento entre as máquinas virtuais.

9. Referências

[1] Adams, K., & Agesen, O. (2006). A comparison of software and hardware techniques for x86 virtualization. *Architectural Support for Programming Languages and Operating Systems* , 2-13.

[2] Carissimi, Alexandre. (2008). Virtualização: da teoria a soluções. *Minicursos do Simpósio Brasileiro de Redes de Computadores - SBRC´2008*, 173-207

[3] Dragovic, B., Fraser, K., Hand, S., Ho, T. H., & Pratt, I. (2003). Xen and the Art of Virtualization. *Proceedings of the ACM Symposium on Operating Systems Principles* .

[4] Jeremy Sugerman, G. V.-H. (2001). Virtualizing I/O Devices on VMware Workstation's Hosted Virtual Machine Monitor . *Proceedings of the 2001 USENIX Annual Technical Conference*.

[5] Menascé, Daniel A.: Virtualization: Concepts, Applications, and Performance Modeling. Int. CMG Conference 2005: 407-414

[6] Rose, Robert: Survey of System Virtualization Techniques. (http://citeseer.ist.psu.edu/rose04survey.html) Acessado em junho 2008.

[7] Quétier, B., Neri, V., & Cappello, F. (Setembro de 2006). Scalability Comparison of Four Host Virtualization Tools. *Journal of Grid Computing* , 83-98.

[8] Uhlig, R. N., Bennett, S., Kagi, A., Leung, F., & Smith, L. (2005). Intel virtualization technology. *Computer* , 48- 56.

[9] VMWare (2008) A Performance Comparison of Hypervisors (http://www.vmware.com). Acesso junho 2008.

[10] VMware, Inc (2008). VMware: Virtualization, Virtual Machine & Virtual Server Consolidation – VMware. (http://www.vmware.com/) Acessado em junho 2008 .

[11] VMware, Inc (2007). Understanding Full Virtualization, Paravirtualization, and Hardware Assist (http://www.vmware.com/). Acessado em junho 2008 .

[12] Xen Source (2008) A Performance Comparaison of Commercial Hypervisors (http:/blogs.xensources.com/rogerk/wp-content/uploads/2007/03/hypervisor_performance_ comparaison_1_0_5_with_esx-data.pdf). Acesso junho 2008.

[13] Xen.org Project (2008). The Official Xen.org Project Site. (http://www.xen.org/) Acessado em junho 2008.