



**MEC – SETEC**  
**SERVIÇO PÚBLICO FEDERAL**  
**INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE MATO**  
**GROSSO**  
**CAMPUS CUIABÁ**  
**DIRETORIA DE PESQUISA E PÓS-GRADUAÇÃO**

## **TÉCNICAS DE VIRTUALIZAÇÃO E SUAS IMPLEMENTAÇÕES**

DEL BARCO NISHIOKA, Eder

Orientador: André Valente do Couto

**RESUMO:** Atualmente a virtualização é utilizada como uma solução para fornecer alguns benefícios a determinados sistemas. Neste artigo serão abordados conceitos que permeiam as técnicas de virtualização, bem como serão vislumbrados algumas implementações da virtualização. Ainda, será feita uma análise comparativa com o intuito de identificar o melhor uso dessas implementações.

**ABSTRACT:** Currently, virtualization is used as a solution to provide some benefits to certain systems. This paper will be discussed concepts that permeate the virtualization techniques, as well as be glimpsed some implementations of virtualization. Still, there will be a comparative analysis in order to identify the best use of these implementations.

### **1 INTRODUÇÃO**

A virtualização não é um processo ou idéia nova tendo sua implementação sido realizada há mais de 30 anos pela IBM como uma forma de particionar logicamente os computadores mainframe em máquinas virtuais separadas para otimização do seu uso. Essas partições permitiam aos mainframes executar várias tarefas, vários aplicativos e processos ao mesmo tempo.

A virtualização então surgiu como forma de aprimorar a utilização dos recursos de TI com o foco na entrega dos serviços e não mais na utilização exclusiva de determinados recursos, proporcionando às empresas a: consolidação de sua infra-estrutura, otimização do uso do hardware, economia com energia elétrica e flexibilidade de sua infra-estrutura para atender suas eventuais necessidades.

Algumas implementações fizeram possível o uso desta tecnologia em ambiente mais disseminado, sendo que no ano de 2003 o XEN, software que implementa técnicas de virtualização, foi criado através de um projeto de pesquisa da universidade de Cambridge. No mesmo ano a Microsoft, adquiriu uma empresa que estava no mercado desde 1988 chamada Connectix e com esta base lançou em 2004 o Virtual PC e em 2008, juntamente com o lançamento do Sistema Operacional Windows Server 2008, foi incorporado sua solução de virtualização o Hyper-V. Ainda, na década de 90, a VMware criou um produto líder no segmento de virtualização para a plataforma x86.

## **2. DEFINIÇÕES E CONCEITOS**

O objetivo principal da virtualização está, no compartilhamento otimizado de todos os recursos disponíveis. Todo o gerenciamento dos recursos virtualizados são realizados utilizando-se os conceitos de: Instruções Privilegiadas e não privilegiadas, sendo que essas instruções fazem parte do conjunto de instruções da arquitetura x86.

Esta classificação se faz necessária considerando que 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 e as instruções privilegiadas podem alterar o estado e a alocação desses recursos.

Um computador opera 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.

A arquitetura de virtualização abordada neste artigo é a x86, e neste contexto, existem quatro níveis de privilégio, que são chamados de *anéis*. Os *anéis* 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 hospedeiros são executados com esse nível de privilégio, enquanto que os sistemas operacionais visitantes são executados nos outros níveis

O 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 (*Guest 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 *SO visitantes* simultaneamente.

Os *SO hospedeiros* são controlados e a utilização de seus recursos são gerenciados por uma camada de software denominada *VMM (Virtual Machine Manager)*. O *Virtual Machine Monitor (VMM)* segundo (Whitaker, 2004) é uma camada de software que suporta a execução concorrente de múltiplas máquinas virtuais.

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.

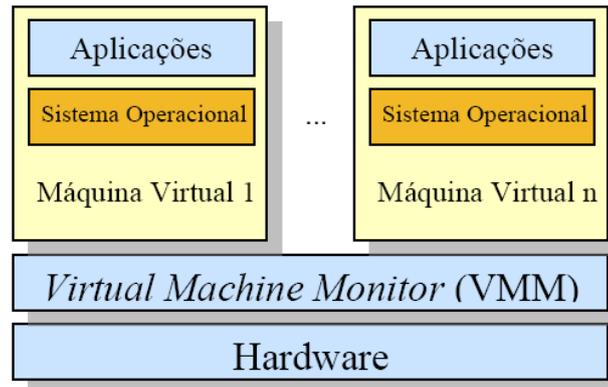


Figura 1. Relacionamento das Máquinas Virtuais e do VMM.  
Fonte: MATTOS, 2010.

### 3. VIRTUALIZAÇÃO TOTAL E PARAVIRTUALIZAÇÃO

A abordagem de implementação do *VMM* pode ser realizada principalmente por duas formas, a saber: virtualização total ou paravirtualização.

A virtualização total tem por objetivo fornecer ao sistema operacional visitante uma réplica do hardware subjacente. O sistema operacional visitante é executado sem modificações sobre o monitor de máquina virtual (*VMM*). Ocorre aqui uma desvantagem em seu desempenho, pois o número de dispositivos a serem suportados pelo *VMM* é extremamente elevado. Para resolver isto as implementações da virtualização total usam dispositivos genéricos, que por um lado funcionam bem para a maioria dos dispositivos disponíveis e por outro não sacrificam a eficiência na utilização dos recursos resultando em uma degradação na performance.

A virtualização total tem que contornar alguns problemas gerados pela implementação dos sistemas operacionais, já que esses foram implementados para executarem como instância única nas máquinas físicas, não disputando recursos com outros sistemas operacionais. Um exemplo: 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.

A para-virtualização é uma alternativa à virtualização total. Nela 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.

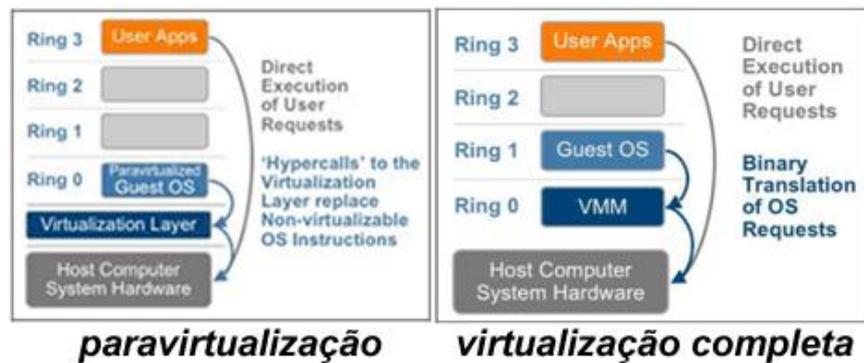


Figura 2. Virtualização Total e ParaVirtualização Arquitetura x86.  
Fonte: MATTOS, 2010.

Embora a para-virtualização apresente um ganho de desempenho significativo frente à virtualização total, essa disparidade tem sido superada devido à presença de instruções de virtualização nos processadores que favorecem a virtualização total.

Dentre os maiores fornecedores de processadores que disponibilizam instruções de virtualização diretamente em seus chips, temos a: a IVT (Intel Virtualization Technology) codinome Vanderpool da Intel e a AMD-V (AMD-Virtualization), codinome Pacífica da AMD.

Embora tenham sido desenvolvidas para o mesmo propósito, foram projetadas de maneira independentes. Por esse motivo, há alguns problemas na portabilidade de máquinas virtuais entre essas plataformas (arquitetura Intel para a arquitetura AMD e vice-versa).

#### 4. FERRAMENTAS DE VIRTUALIZAÇÃO

Aqui serão abordadas as três principais ferramentas de virtualização para a arquitetura x86: o VMWare, o Hyper-V e o Xen. Todos são produtos de mercado, porém possuem algumas diferenças na implementação das técnicas de virtualização. A primeira e mais marcante é o fato do XEN ser um exemplo de

paravirtualização enquanto que o Hyper-V e o VMware serem exemplos de virtualização completa.

#### 4.1. XEN

O *Xen* é um dos mais populares exemplos de paravirtualização. 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*.

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 (Menascé, 2005).

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 (Menascé, 2005).

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 máquinas virtuais dos domínios U têm que acessar através do domínio 0 (Andrade, 2009).

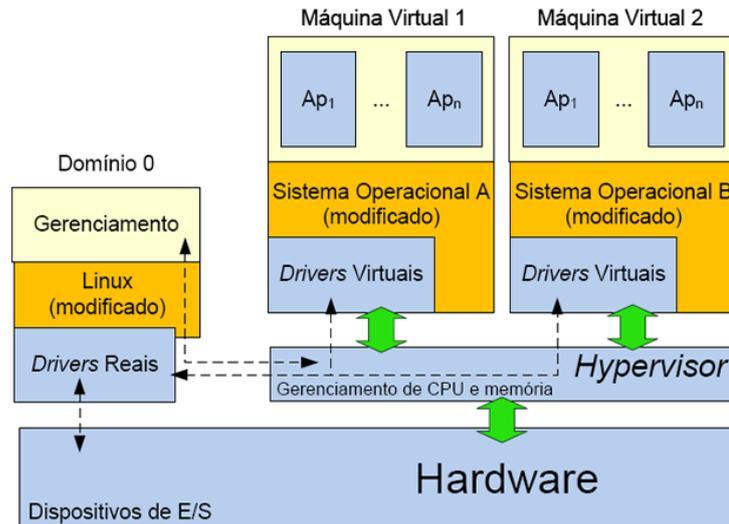


Figura 3. Componentes do XEN: Hypervisor e Domínios.  
Fonte: ANDRADE, 2009.

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 (Quétier, 2006).

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*.

## 4.2. VMWARE

A Arquitetura do VMware compreende no sistema operacional chamado *VMKernel*, e seus processos. O *VMKernel* fornece meios de executar todos os processos do sistema, incluindo gerenciamento de aplicações, gerenciamento dos agentes, bem como de todas as máquinas virtuais. Ele possui o controle de todos os dispositivos de hardware e gerenciamento de recursos das aplicações. Os principais processos que executam no *VMKernel* são: *Direct Console User Interface* (DCUI) Console direto da interface de usuário, *The virtual machine monitor* (VMM) – Monitor de Máquina Virtual, *agents* os agentes e *Common Information Model* (CIM) Modelo de Informação Comum.

O console direto da interface de usuário permite uma configuração de baixo nível e gerenciamento de interface, acessível através do console do servidor, usado na configuração básica inicial. O monitor de máquina virtual, é o processo que fornece a execução de uma máquina virtual, de um processo conhecido como *VMX*, cada máquina virtual executada tem sua própria *VMM* e processo *VMX*. Os agentes são usados para habilitar o mais alto nível de gerenciamento de infra-estrutura de aplicações remotas. O modelo de informação comum é a interface que habilita o gerenciamento de nível do hardware de aplicações remotas através de um conjunto de APIs padrão. (MATTOS, 2010).

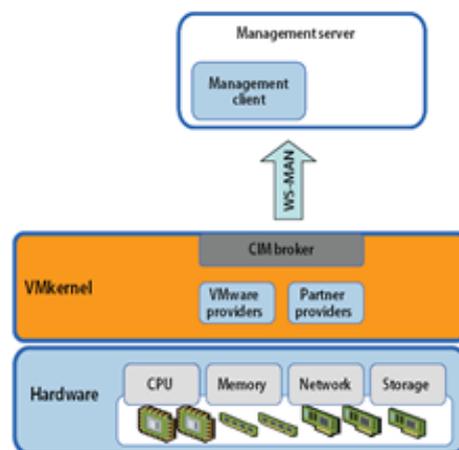


Figura 4. Estrutura básica da VMware.

Fonte: MATTOS, 2010.

### 4.3. HYPER-V

*Hyper-V* é uma tecnologia de virtualização baseada em *hypervisor* para versões do *Windows Server 2008 64 bits*. O *hypervisor* é a plataforma de virtualização que permite que vários sistemas operacionais isolados compartilhem uma única plataforma de hardware (ARUNKUNDRAM, 2010).

A pilha de virtualização roda na partição pai e tem acesso direto aos dispositivos de hardware. A partição pai ou *raiz (root)* cria as partições filho que hospedam os sistemas operacionais convidados. Uma partição pai cria as partições filhos usando o aplicativo *hypercall interface de programação (API)* (ARUNKUNDRAM, 2010).

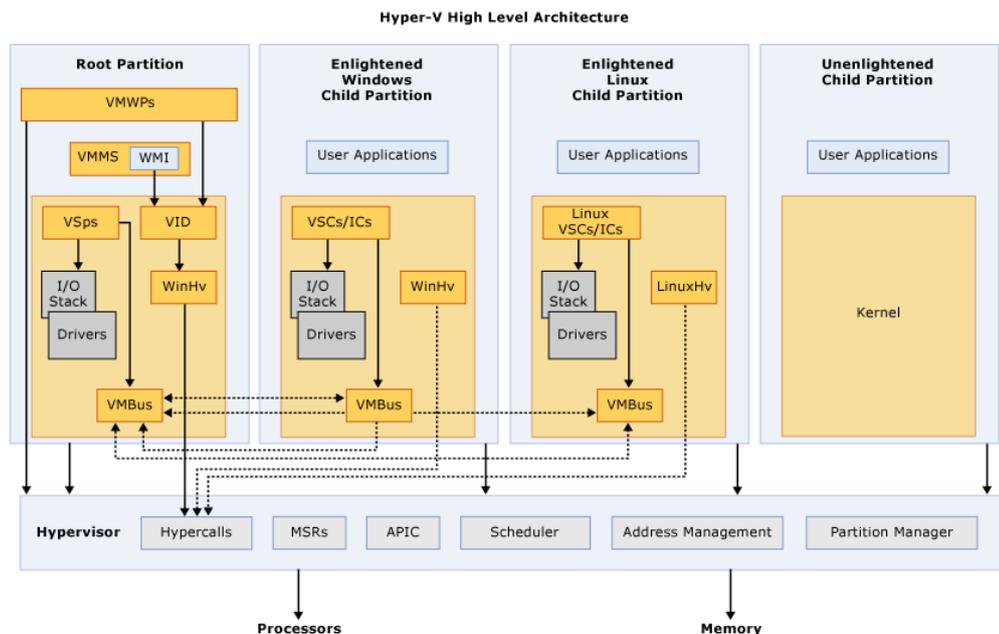
As partições têm uma visão virtual do processador e são executados em uma região de endereço de memória virtual que é privada para cada partição

convidada. O *hypervisor* controla as interrupções do processador, e redireciona para a respectiva partição. As partições filhas não tem acesso direto a outros recursos de hardware e são apresentados uma visão virtual dos recursos, com os dispositivos virtuais (*VDevs*).

As requisições para os dispositivos virtuais são redirecionados, quer através da *VMbus* ou do *hypervisor* para os dispositivos na partição pai, que lida com as solicitações. O *VMbus* é um canal de comunicação lógica inter-partição ([http://msdn.microsoft.com/en-us/library/cc768520\(v=bts.10\).aspx](http://msdn.microsoft.com/en-us/library/cc768520(v=bts.10).aspx), 2011).

Todo esse processo é transparente para o sistema operacional convidado. O *hypervisor kernel* é fornecida através de instalação de serviços de integração Hyper-V, componentes de integração Hyper-V, componentes de integração, que incluem *virtual server client (VSC) drivers* – Drivers de Servidores de Clientes Virtuais que também estão disponíveis para outros sistemas operacionais cliente ([http://msdn.microsoft.com/en-us/library/cc768520\(v=bts.10\).aspx](http://msdn.microsoft.com/en-us/library/cc768520(v=bts.10).aspx), 2011).

O diagrama a seguir fornece uma visão geral de alto nível da arquitetura de um ambiente do *Hyper-V* em execução no *Windows Server 2008*.



**Figura 5. Arquitetura do Hyper V.**

Fonte: [http://msdn.microsoft.com/en-us/library/cc768520\(v=bts.10\).aspx](http://msdn.microsoft.com/en-us/library/cc768520(v=bts.10).aspx), 2011.

## 5. MIGRAÇÃO ENTRE PLATAFORMAS VMWARE E HYPER V

O maior benefício da virtualização de servidores é a capacidade de migrar máquinas virtuais em execução, em máquinas físicas (PRATT, 2005). Isso viabiliza alta disponibilidade dos serviços como também colabora para o balanceamento de carga da utilização feita sobre as máquinas reais. O *Vmware*, o *XEN Enterprise* e o *Hyper-V* realizam este tipo de migração. Porém a abordagem principal será nas implementações de virtualização completa (*Hyper-V* e *VMware*).

O processo de migração do VMware e do Hyper-V são semelhantes, porém cada uma possui suas características próprias. Na figura 5, temos um breve quadro comparativo entre as tecnologias.

Comparison of core VMware vSphere capabilities vs. Microsoft System Center	VMware vSphere 4	Microsoft WS08 Hyper-V R2/ SMSD
Physical and Virtual Management	✗	✓ SMSD
VMware and Microsoft Management	✗	✓ SMSD
In-guest Monitoring	✗	✓
End-to-End OS Monitoring	✗	✓ SMSD OpsMgr
Application/Service Monitoring	✗	✓ SMSD, PRO
End-to-End Process Automation	✗	✓ Opalis
Virtual Machine Lifecycle Management	✗ Sold Separately	✓
IT Service Management	✗ Thru Ionix	✓
Host/Virtual Machine Level Optimization	✓ DRS	✓ SMSD, PRO
Centralized HV Management	✓ vCenter	✓ SMSD, VMM
Guest OS Patching/Management	✓	✓ SMSD, SCCM
Virtual Machine High Availability/Failover	✓ vCenter	✓ WS08 Clustering + VMM
Virtual Machine Migration	✓ vMotion	✓ Live Migration
Storage Virtual Machine Migration	✓	✓ <sup>1</sup>

WS08 = Windows Server 2008  
 PRO = Performance and Resource Optimization  
 SCCM = System Center Configuration Manager  
 VMM = Virtual Machine Manager  
 SMSD = System Center Server Management Suite Datacenter  
<sup>1</sup> Quick

FIGURA 6. Comparação de compatibilidade VMware e Hyper V.

FONTE: <http://www.microsoft.com/virtualization/en/us/microsoft-advantage.aspx>, 2011.

Conforme a figura 5, o gerenciamento do *VMware* possui algumas limitações, sem suporte no que tange ao: gerenciamento físico e virtual, monitoramento fim a fim do sistema operacional, monitoramento de serviço/aplicação, automação de processos fim a fim, gestão do ciclo de vida de máquinas virtuais, gerenciamento do serviço de TI.

O *Hyper-V* por possuir o *SMSD* (*System Center Server Management Suite Datacenter*) e o *SCCM* (*System Center Configuration Manager*), possui então um gerenciamento centralizado de seus serviços. Assim serviços integrados com a

plataforma *Windows*: *SQL Server*, *Hyper-V*, *Active Directory*, entre outros, são consolidados e integrados diretamente.

Já nos serviços de: otimização do nível da máquina virtual hospedeiro; centralização do *hypervisor* centralizado; gerenciamento do patching do sistema operacional convidado; gerenciamento de failover e alta disponibilidade da máquina virtual; migração da máquina virtual e armazenamento de máquina virtual, ambas as tecnologias possuem suporte nestes serviços.

O VMware possui um gerenciamento escalável e extensível quando utiliza o *VCenter* e o *VMotion*, integrando parte de sua estrutura a plataforma virtualizada em específico.

Ambas possuem a opção *live migration* migração ao vivo de máquinas que estão sendo virtualizadas enquanto estão em pleno processamento de dados. Assim ambas tecnologias possuem vantagens e desvantagens sobre a outra, e analisar qual é mais específica para determinada infra-estrutura é o fator primordial para se determinar qual delas é mais adequada para ser utilizada. Compreende-se então que o Hyper-V é interessante em ambientes totalmente *Microsoft* enquanto que o VMware em ambientes de alta disponibilidade e de multiplataforma.

## 6. CONCLUSÃO

Virtualização é uma técnica que está cada vez mais presente na área de TI. inúmeras empresas estão investindo em soluções de gerência de ambientes virtualizados e pelo aumento sucessivo nos investimento na área. 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. Qual tecnologia utilizar, será determinada conforme as aquisições da infra-estrutura, para ser adequada a cada estrutura em específico.

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.

Existem questões que ainda não estão completamente resolvidas, tais como a migração de máquinas virtuais entre diferentes tecnologias, portabilidade e gerenciamento entre diferentes plataformas, computação em nuvem híbrida, gerenciamento de recursos pelo *hypervisor*, gerenciamento de memória, gerenciamento de disco, gerenciamento dos agentes das máquinas virtuais entre outros temas para eventuais trabalhos futuros.

## REFERÊNCIAS

- ARUNKUNDRAM, Rajiv. **Uma introdução ao Hyper-V no Windows Server 2008**. Disponível em: <http://technet.microsoft.com/pt-br/magazine/cc895595.aspx>. Acessado em: setembro 2010.
- ANDRADE, Marcos Tadeu. **Um estudo comparativo sobre as principais ferramentas de virtualização**. Pernambuco. Disponível em (<http://www.cin.ufpe.br/~tg/2006-2/mta.pdf>). Acessado em: setembro de 2010.
- INTEL. Página da empresa Intel. Disponível em: <http://www.nextg.com.br/v3/web/curso.php>. Acesso em: Junho de 2011.
- LAUREANO, Marcos. **Máquinas Virtuais e Emuladores**. 1.ed. São Paulo: Editora Novatec Ltda, 2006. 30 p.
- LAUREANO, Marcos; MAZIERO, Carlos; JAMHOUR, Edgard. **Proteção de detectores de intrusão através de máquinas virtuais, 2004**. Disponível em: <http://www.mlaureano.org/projetos/deteccao-de-intrusao-em-maquinas-virtuais>. Acesso em: Novembro. 2010.
- MATTOS, Diogo Menezes Ferazani. **Virtualização: VWare e Xen**. Disponível em: [http://www.gta.ufrj.br/grad/08\\_1/virtual/artigo.pdf](http://www.gta.ufrj.br/grad/08_1/virtual/artigo.pdf). Acessado em: setembro de 2010.
- MANASCÉ, Daniel A.: **Virtualization: Concepts, Applications, and Performance Modeling**. Int. CMG Conference 2005: 407-414
- PRATT, A. W. . C. L. . S. H. . K. F. I. **Xen 3.0 and the art of virtualization**. Linux Symposium, p. 65–77, 2005.  
[http://msdn.microsoft.com/en-us/library/cc768520\(v=bts.10\).aspx](http://msdn.microsoft.com/en-us/library/cc768520(v=bts.10).aspx), acessado em 20/05/2011.
- Quétier, B., Neri, V., & Cappello, F. (Setembro de 2006). **Scalability Comparison of Four Host Virtualization Tools**. Journal of Grid Computing , 83-98.
- WHITAKER, Andrew. **Building Robust Systems With Virtual Machine Monitors**, 2004, Washington (Estados Unidos).