

**CENTRO PAULA SOUZA**

GOVERNO DO ESTADO DE  
**SÃO PAULO**

**Faculdade de Tecnologia de Americana  
Curso de Análise de Sistemas e Tecnologia da Informação**

## **VIRTUALIZAÇÃO DE SERVIDORES**

**Robson Luiz Garbellotto Fogaça**

**Americana – SP**

**2010**

## **VIRTUALIZAÇÃO DE SERVIDORES**

**Robson Luiz Garbellotto Fogaça**

robson.fogaca@fatec.sp.gov.br

Monografia apresentada à Faculdade de Tecnologia de Americana, para graduação no Curso Superior de Análise de Sistemas e Tecnologia da Informação.

Orientador(a): Prof. Lincon Peretto

**Americana – SP**

**2010**

## **VIRTUALIZAÇÃO DE SERVIDORES**

**Robson Luiz Garbellotto Fogaça**

Monografia aprovada em 02/12/2010 para obtenção do título de Tecnólogo em Análise de  
Sistemas e Tecnologia da Informação

Banca Examinadora

Professor Orientador: Lincon Peretto

Professor Convidado: Benedito Aparecido Cruz

Professor Convidado: Rogério Nunes de Freitas

## **AGRADECIMENTO**

Em primeiro lugar agradeço à Deus pela bondade e misericórdia em me permitir cursar uma faculdade pública e reconhecida perante a sociedade e meios acadêmicos, dando-me saúde e forças.

Agradeço também à minha querida mãe Zenaide, que sempre esteve ao meu lado em todos os momentos.

Agradeço à minha noiva Karina, que foi a maior incentivadora para que eu continuasse nessa caminhada árdua, porém, gratificante.

Agradeço aos meus irmãos, que sempre se mostraram solidários e compreensivos nesse período de estudos.

E agradeço também à todos os meus professores, que nunca se cansaram de me mostrar os caminhos mais seguros e corretos durante essa jornada, dando-me todo o conhecimento que tanto faz a diferença em nossa vida, e em especial ao professor e amigo Lincon Peretto, que me orientou com muita dedicação e boa vontade.

Por fim, agradeço a todos os meus colegas de classe, que participaram dessa caminhada tão importante em nossas vidas.

## RESUMO

Esta monografia teve por objetivo estudar a virtualização de servidores, bem como as tecnologias existentes para esta finalidade. Fazendo um comparativo entre um sistema computacional tradicional e um sistema computacional virtualizado, observando suas diferenças e identificando as ferramentas mais eficazes para a virtualização. Dentre as máquinas virtuais, existem dois modelos, conhecidos como máquinas virtuais clássicas ou do Tipo I e máquinas virtuais Hospedadas ou do Tipo II. Ambos os modelos são utilizados para a virtualização de servidores, sendo que a máquina virtual do Tipo I destina-se à virtualização direta no hardware enquanto a máquina virtual do Tipo II destina-se à virtualização no sistema anfitrião, isto é, um sistema operacional. Dentre as diversas ferramentas de virtualização existentes, quatro foram apresentadas neste trabalho, sendo que a ferramenta VMware foi o foco deste estudo. A ferramenta VMware conta com diversas versões de máquinas virtuais onde cada uma delas é utilizada para uma finalidade específica, porém, ambas para a virtualização. Além de versões de máquinas virtuais diferentes, a VMware possui diversos produtos que possibilitam que a virtualização de servidores possam ser implementadas de maneira segura e ágil, contando com produtos que promovem alta disponibilidade, fácil gerenciamento e custo reduzido quando comparado com uma infra-estrutura convencional de ambiente de TI.

Palavras chaves: Virtualização, Servidores, Máquinas Virtuais

## **ABSTRACT**

This monograph has been for objective studying the virtualization of servers as well as existing technologies for this purpose. Making a comparison between a traditional computer system and a virtualized computing system, noting their differences and identifying the most effective tools for virtualization. Among the virtual machines, there are two models, known as virtual machines classic or Type I and virtual machines Hosted or Type II. Both models are used for server virtualization, where virtual machine of Type I is destined to on the hardware virtualization virtual machine while Type II is intended for virtualization in the host system, an operating system. Among the several virtualization tools available, four were presented in this work, and the VMware tool was the focus of this study. The tool has several versions VMware virtual machines where each is used for a specific purpose, however, both for virtualization. In addition to different versions of virtual machines, VMware has several products that enables server virtualization can be implemented safely and agile, with products that promote high availability, easy manageability and low cost compared to a conventional infrastructure the IT environment.

Keywords: Virtualization, Servers, Virtual Machines

## LISTA DE ILUSTRAÇÕES

<b>Figura 1 - Representação dos componentes dos sistemas tradicionais.....</b>	<b>14</b>
<b>Figura 2 - Esquema representativo de máquinas virtuais do tipo I.....</b>	<b>16</b>
<b>Figura 3 - Esquema representativo de máquinas virtuais do tipo II.....</b>	<b>17</b>
<b>Figura 4 - Representação da estrutura do VMware HA.....</b>	<b>27</b>
<b>Figura 5 - Representação da estrutura do VMware DRS.....</b>	<b>33</b>
<b>Figura 6 - Representação da estrutura do VMware VMotion.....</b>	<b>36</b>
<b>Figura 7 - Representação da estrutura do VMware Consolidated Backup.....</b>	<b>39</b>
<b>Figura 8 - Representação da estrutura do VMware vSTORAGE VMFS.....</b>	<b>43</b>

## SUMÁRIO

1.	INTRODUÇÃO.....	9
2.	VIRTUALIZAÇÃO .....	10
2.1.	MODELO TRADICIONAL.....	10
2.2.	SISTEMA OPERACIONAL / HARDWARE.....	10
2.3.	PROCESSO, INSTRUÇÃO, NÍVEIS DE ABSTRAÇÃO E INTERFACE.....	11
2.3.1.	PROCESSO .....	11
2.3.2.	INSTRUÇÕES .....	11
2.3.3.	INSTRUÇÕES DE VIRTUALIZAÇÃO.....	12
2.3.4.	NÍVEIS DE ABSTRAÇÃO E INTERFACE .....	13
2.4.	MODELO VIRTUALIZADO .....	15
2.4.1.	SISTEMA OPERACIONAL / HARDWARE.....	15
2.4.2.	MÁQUINAS VIRTUAIS CLÁSSICAS ou TIPO I.....	15
2.4.3.	MÁQUINAS VIRTUAIS HOSPEDADAS ou TIPO II.....	16
2.4.4.	HYPERVISOR .....	17
2.5.	MODELO PARAVIRTUALIZADO .....	17
2.6.	LINHAS DE DESENVOLVIMENTO – INTEL E AMD .....	18
2.7.	ARMAZENAMENTO .....	19
2.7.1.	HD EXTERNO.....	20
2.7.2.	FITAS DAT .....	20
2.7.3.	STORAGE.....	20
3.	FERRAMENTAS.....	22
3.1.	VMWARE.....	22
3.1.1.	VIRTUALIZAÇÃO EM DISCO .....	22
3.1.2.	VIRTUALIZAÇÃO DA MEMÓRIA .....	22
3.1.3.	VIRTUALIZAÇÃO DE REDE.....	23
3.1.4.	VMWARE SERVER.....	23
3.1.5.	VMWARE WORKSTATION.....	24
3.1.6.	VMWARE PLAYER .....	24
3.1.7.	VMWARE HA (HIGH AVAILABILITY) .....	24
3.1.8.	VMWARE DRS (DISTRIBUTED RESOURCE SCHEDULER).....	27
3.1.9.	VMWARE VMOTION .....	33
3.1.10.	VMWARE VCB – CONSOLIDATED BACKUP.....	36
3.1.11.	VMWARE vSTORAGE VMFS.....	39
3.1.12.	LINHA DE COMANDO.....	43
3.1.13.	SUPORTE VIA SSH.....	44
3.2.	VIRTUAL BOX .....	46
3.3.	XEN.....	48
3.4.	VIRTUAL PC.....	49
4.	CONCLUSÃO.....	50
5.	REFERÊNCIAS BIBLIOGRÁFICAS .....	52



## 1. INTRODUÇÃO

A virtualização foi desenvolvida na década de 60 com a finalidade de particionar os hardwares dos grandes mainframes, no intuito de alcançar a sua melhor utilização. Nessa época, a virtualização foi implantada pela IBM. Nos anos 90 a VMware desenvolveu a virtualização para plataforma x86 com a finalidade de solucionar sua subutilização e outros problemas. Atualmente, a VMware é a grande líder no segmento de ferramentas para virtualização.

Além da VMware, existem outras ferramentas de virtualização, como o Xen, Virtual Box, Hyper-V, entre outros.

Devido o fato de a VMware ter se tornado o ícone para virtualização de servidores, mesmo sendo um software proprietário, o foco deste estudo baseou-se nessa ferramenta.

Suas principais versões são VMware ESX Server, VMware Server, VMware Workstation e também VMware Player.

Bem como máquinas virtuais, a VMware possui diversos produtos, como VMware HA (*High Availability*), que proporciona alta disponibilidade para o ambiente computacional, o VMware DRS (*Distributed Resource Scheduler*), que tem a função de equilibrar de forma dinâmica a capacidade computacional entre um conjunto de recursos de hardware agregados em um pool lógico de recursos, e também o VMware vMotion, que permite a migração em tempo real de máquinas virtuais em execução de um servidor físico para outro, sem tempo de inatividade.

Todos esses recursos permitem manter um ambiente computacional completo com redução considerável de custos e espaço físico, uma vez que em apenas um servidor físico é possível conter vários servidores lógicos, com as mesmas características e funções.

Este trabalho tem como objetivo apresentar as inovações da virtualização, seus conceitos, sua funcionalidade, suas diferenças entre as demais características, além de um comparativo entre um modelo computacional tradicional, com seu sistema operacional, hardware, seus processos, instruções, níveis de abstração e interface, e o modelo virtualizado, que incluem as máquinas virtuais clássicas ou do tipo I e as máquinas virtuais hospedadas ou do tipo II.

Será apresentado também o modelo paravirtualizado, com suas definições e as linhas de desenvolvimento da Intel e AMD e tipos de armazenamento.

## **2. VIRTUALIZAÇÃO**

Virtualização refere-se às tecnologias desenvolvidas para fornecer uma camada de abstração entre sistemas de hardware de computador e o software que é utilizado nestes sistemas. A virtualização possibilita o uso de diversos sistemas operacionais executando simultaneamente em uma única máquina. Afirmamos que uma máquina virtual é um ambiente operacional completo que se comporta como uma máquina independente.

O início do uso de máquinas virtuais se deu na década de 60, quando houve a necessidade de particionar de maneira lógica os mainframes, tornando-os máquinas virtuais separadas. Com essas partições, os mainframes puderam assumir múltiplas tarefas, assim executando vários aplicativos e processos ao mesmo tempo.

Entre as décadas de 80 e 90, quando os aplicativos de servidores-clientes, servidores e desktops x86 baratos contribuía para a computação distribuída, houve o abandono da virtualização. A adoção ampla do Windows e o surgimento do Linux como sistemas operacionais de servidor, na década de 90, estabeleceram os servidores x86 como o padrão do setor.

Aos poucos, o conceito de virtualização foi tornando-se forte e nos dias atuais estão presentes numa grande parte das empresas, corporações, entre outros, principalmente de tecnologias de informação.

### **2.1. MODELO TRADICIONAL**

### **2.2. SISTEMA OPERACIONAL / HARDWARE**

No modelo tradicional, um sistema computacional pode ser entendido como um conjunto de hardware no qual existe uma série de funções (aplicações) que podem ser executadas. Uma aplicação é um conjunto de funções que permite a realização de uma tarefa para um usuário. Essas funções podem ser executadas se o hardware subjacente for projetado para atendê-las.

A divisão de recursos é feita por um software no nível abaixo das aplicações, conhecido como sistema operacional. Sistemas operacionais são camadas de software, que ficam entre o hardware e as aplicações, que são capazes de orientar a utilização desses recursos físicos. A idéia

é otimizar essa utilização. Sua responsabilidade é organizar o uso da máquina criando abstrações como, por exemplo, um arquivo. Um arquivo não é algo físico, mas sim uma abstração no nível do usuário que corresponde a um grupo específico de bits armazenados em um local físico determinado. Essa abstração de recursos para que o usuário possa usar a máquina através de uma interface amigável é chamada virtualização de recursos. Com a utilização dessa técnica, cada programa tem a confortável ilusão de estar sendo executado sozinho, enquanto na verdade está dividindo os recursos da máquina com outras aplicações simultâneas.

Ao falar de um modelo tradicional, é importante frisar os termos Processos, Instruções, Níveis de abstração e interface.

## **2.3. PROCESSO, INSTRUÇÃO, NÍVEIS DE ABSTRAÇÃO E INTERFACE.**

### **2.3.1. PROCESSO**

Um processo é definido como a representação de um programa. Trata-se basicamente de uma abstração que reúna os dados a serem manipulados pelo programa e as suas funções usadas. O processo é implementado pela representação de um espaço de endereçamento lógico divididos em regiões que guardam informações específicas.

A execução de um processo é realizada através de dois registradores: PC (Program Counter - Contador de Programa), que indica a função a ser executada, e SP (Stack Pointer - Apontador de Pilha), que mostra onde devem ser guardados, no processo, os dados de retorno dessa função, seus parâmetros e suas variáveis locais.

### **2.3.2. INSTRUÇÕES**

Sobre as instruções, todas as tarefas realizadas por um sistema computacional devem ser traduzidas em funções mais básicas, para que os recursos físicos sejam capazes de executar. Essas funções mais básicas recebem o nome de instruções.

As instruções são conjuntos de bits que representam comandos para a máquina. O protocolo que define como os bits são organizados para que tenham um significado é o que

permite que a máquina reconheça a tarefa desejada. Os programas, ao serem criados em uma linguagem de programação, precisam que suas tarefas sejam traduzidas em instruções para a máquina, e isso é feito pela compilação.

Deste modo, todo hardware corresponde a um conjunto de instruções (ISA) que deverá utilizar todos os seus recursos. O conjunto de instruções pode ser entendido, portanto, como uma interface entre a camada de software e o hardware.

Existe um conceito de divisão entre as instruções importantes e essenciais para o emprego da virtualização: instruções privilegiadas e instruções não privilegiadas. As instruções privilegiadas são aquelas que alteram recursos compartilhados entre vários processos, como registradores especiais e memória principal. As não-privilegiadas podem ser executadas sem que nenhum recurso usado por outro programa seja alterado.

Partindo-se dessa divisão entre as instruções, é criada uma divisão para o modo de uso de um computador entre modo de usuário e modo de supervisor. O modo de usuário, também chamado de espaço de aplicação, fica restrito apenas em gerar instruções não-privilegiadas, o que exime o usuário da responsabilidade de não gerar instruções que prejudiquem o funcionamento do sistema. Já o modo de supervisor tem um total controle sobre a CPU, podendo executar qualquer tipo de instrução.

A instrução que será executada na CPU fica armazenada, em forma de bits, em um registrador especial, o PC. Esse registrador indica em última análise, portanto, o que a CPU deve fazer naquele momento, e trabalha em conjunto com outro registrador, o apontador de pilha (SP), que passa parâmetros para certa tarefa. Cada programa, entretanto, tem uma instrução a ser executada. Na verdade, um processo tem dois registros que comandam sua execução, o apontador de pilha e o contador de programa. Eles representam a CPU que o programa acredita estar usando, a CPU virtual. Para executar, o programa precisa que esses dois registros sejam passados à CPU real, da máquina.

Para resolver o problema de vários programas tentarem usar a CPU ao mesmo tempo, o sistema operacional utiliza uma técnica chamada escalonamento. Isso consiste em compartilhar o uso da CPU entre os processos, de forma que os processos tenham a ilusão de estarem usando sozinho a máquina.

### **2.3.3. INSTRUÇÕES DE VIRTUALIZAÇÃO**

Para que uma arquitetura possa ser virtualizada, é necessário que todas as instruções privilegiadas sejam disponibilizadas para o modo supervisor quando originadas em modo usuário. No entanto, em arquiteturas como a x86, o kernel do sistema convidado poderá estar executando em modo usuário, pelo fato de poder estar utilizando instruções assembler que não podem ser capturadas e emuladas. Essa arquitetura possui diversas instruções que tem comportamento diferente no modo usuário e supervisor, por isso, não causam uma exceção na CPU. Um bom exemplo disso é que uma aplicação em modo usuário poderia perguntar se ela está executando em modo supervisor ou em modo usuário, e obteria a mesma resposta: “modo usuário”, sem qualquer chance do monitor de máquinas virtuais interceptar essa instrução e retornar uma resposta falsa [STEIL]. Desta forma, pode-se afirmar que a arquitetura x86 não é estritamente virtualizável, pois não possui nativamente um modo hipervisor e nem todas as instruções sensíveis causam traps de CPU. Esse problema pode ser contornado da seguinte maneira, em algumas soluções o código x86 é analisado instrução por instrução e emulado, entretanto, este processo causa uma perda de desempenho considerável. Esta técnica também é conhecida como emulação do código x86 e é utilizada pelo software de virtualização Bochs. Em outras soluções é utilizada uma técnica chamada tradução binária (ou reescrita binária), que é bem mais eficiente em termos de desempenho. Essa técnica atualmente é a mais utilizada e são implementados em softwares como VMware, Microsoft Virtual Server e outros.

#### **2.3.4. NÍVEIS DE ABSTRAÇÃO E INTERFACE**

Para os níveis de abstração e interface, a divisão de um sistema computacional em diversos níveis de abstração é um princípio básico e muito importante. Cada nível de abstração realiza a troca de informações com os níveis vizinhos sem a necessidade de saber como essas informações são tratadas pelos outros níveis. Para isso acontecer é necessário a interposição de uma interface entre os níveis.

Os níveis de abstração podem ser divididos em aplicação, bibliotecas, sistema operacional e processador.

O nível de aplicação é responsável por executar a aplicação desejada pelo usuário, possivelmente trocando informações com o mesmo. As bibliotecas são conjuntos de funções usadas pelo programador para fazer o programa acessar recursos protegidos da máquina. Isso permite que bibliotecas sejam criadas com o objetivo de fornecer aos programadores funções que gerem instruções privilegiadas. As instruções não-privilegiadas geradas pela aplicação atuam diretamente no processador, enquanto as privilegiadas são tratadas pelas bibliotecas. Ao tentar usar recursos protegidos do sistema, a aplicação se comunica com a biblioteca pela Interface Aplicativa de Programação (API).

O terceiro nível, o sistema operacional, se encarrega de executar as instruções não privilegiadas de forma a otimizar a utilização de recursos da máquina. A biblioteca, encarregada de fazer o primeiro tratamento desse tipo de tarefa, usa as “chamadas de sistema” para pedir auxílio ao sistema operacional e usar recursos de hardware. As chamadas de sistema são, assim, a interface entre Bibliotecas e Sistema Operacional.

O nível de processador é o principal, onde o computador realiza seus cálculos. Tudo o que acontece nos outros níveis serve para simplificar o uso do sistema através de instruções, que o processador entende. O conjunto de instruções não-privilegiadas pode ser usado diretamente por todos os níveis acima. O conjunto de instruções privilegiadas, porém, só pode ser usado pelo sistema operacional. Esses dois conjuntos são as interfaces entre o processador e os outros níveis.

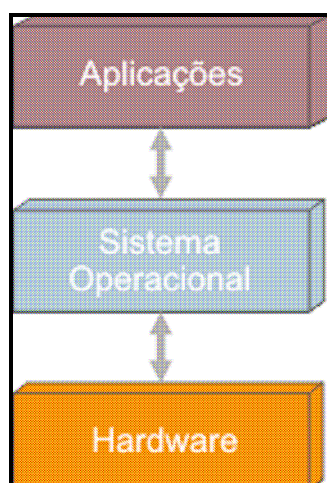


Figura 1. Representação dos componentes dos sistemas tradicionais  
Fonte: Bruno Kinoshita

## **2.4. MODELO VIRTUALIZADO**

### **2.4.1. SISTEMA OPERACIONAL / HARDWARE**

Existem dois tipos de máquinas virtuais, denominadas como MÁQUINAS VIRTUAIS CLÁSSICAS ou do Tipo I e MÁQUINAS VIRTUAIS HOSPEDADAS ou do Tipo II.

Para ambas as máquinas virtuais, existem uma peça chave em seu funcionamento, que são os monitores de máquinas virtuais (VMM), também conhecido com Hypervisor, que será apresentado com maiores detalhes mais abaixo.

### **2.4.2. MÁQUINAS VIRTUAIS CLÁSSICAS ou TIPO I**

Para a máquina virtual clássica ou do tipo I, o monitor será implementado entre o hardware e os sistemas convidados. O monitor realiza o controle sobre o hardware e cria um ambiente de máquinas virtuais dando a cada máquina virtual o comportamento de uma máquina física, devendo executar sobre esses ambientes, sistemas operacionais iguais ou diferentes, totalmente isolados entre si. Esse tipo de monitor executa com maior prioridade sobre os sistemas convidados de maneira que ele pode interceptar e emular todas as operações que acessam ou manipulam os recursos de hardware provenientes dos sistemas convidados.

Nos monitores de tipo I, o sistema convidado acessa diretamente o hardware, onde nesse processo são necessários que sejam realizadas alterações no sistema operacional para que suporte a otimização.

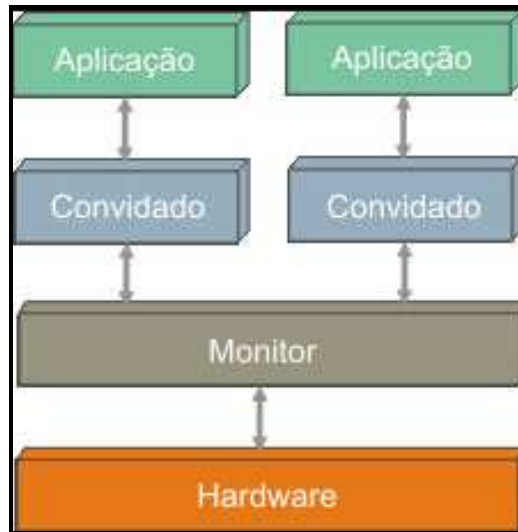


Figura 2. Esquema representativo de máquinas virtuais do tipo I  
 Fonte: Bruno Kinoshita

### 2.4.3. MÁQUINAS VIRTUAIS HOSPEDADAS ou TIPO II

As máquinas virtuais do tipo II recebem a implementação do monitor como um processo de um sistema operacional real, nesse caso o sistema anfitrião.

O monitor do tipo II age de forma analógica ao monitor de tipo I, onde a diferença está no fato de ele ser executado sobre o sistema operacional anfitrião, como se fosse um processo. Neste modelo o monitor simula todas as operações que o sistema anfitrião simularia.

Os monitores do tipo II permitem que o sistema convidado acesse diretamente o sistema anfitrião.

O sistema convidado acessa diretamente o hardware, onde essa otimização é conseguida quando o monitor permite o acesso direto a drivers de dispositivos do sistema anfitrião.

O monitor também acessa diretamente o hardware, de forma que o monitor tenha seus próprios drivers de dispositivos acessando o hardware com uma interface própria, como baixo nível.



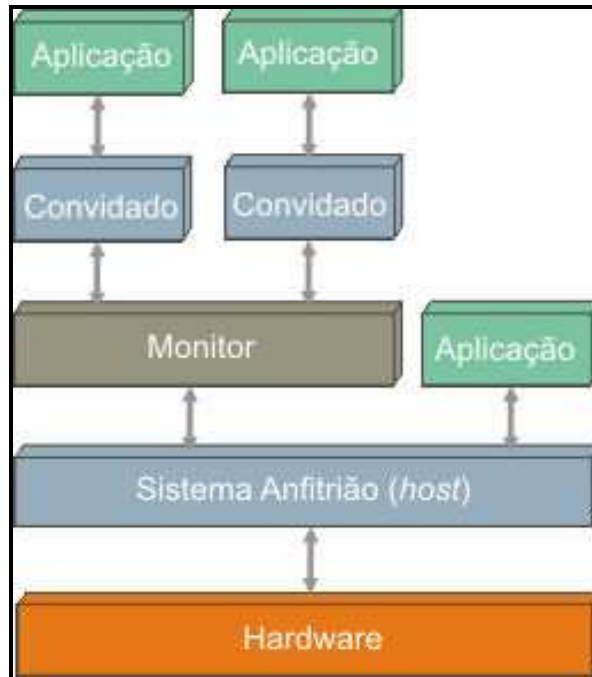


Figura 3. Esquema representativo de máquinas virtuais do tipo II  
 Fonte: Bruno Kinoshita

#### 2.4.4. HYPERVISOR

O hypervisor, também conhecido como Monitor de Máquina Virtual (VMM), é uma camada de software existente 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. Vale lembrar 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.

Hypervisor é o componente mais básico da virtualização. É o software que desvincula o sistema operacional e os aplicativos de seus recursos físicos. Um hipervisor tem seu próprio kernel e é instalado diretamente no hardware, ou “bare metal”. (Ele é, quase literalmente, inserido entre o hardware e o sistema operacional).

#### 2.5. MODELO PARAVIRTUALIZADO

Paravirtualização é definida como um tipo de virtualização em que o sistema operacional completo roda sobre o hipervisor e realiza uma comunicação direta com ele, provendo uma melhor performance. Entretanto, os kernels do sistema operacional e do hipervisor necessitam ser modificados para acomodar esta interação estreita. Um sistema operacional Linux paravirtualizado, por exemplo, é otimizado especificamente para rodar em um ambiente virtual. A virtualização total, em comparação, apresenta uma camada abstrata que intercepta todas as chamadas para recursos físicos. A paravirtualização se baseia num subconjunto virtualizado da arquitetura x86. Avanços recentes em chips da Intel e da AMD estão ajudando a suportar esquemas de virtualização que não requerem sistemas operacionais modificados. “Vanderpool”, a tecnologia de virtualização da Intel no nível do chip, foi uma das primeiras inovações deste tipo. A extensão “Pacifica” da AMD provê suporte adicional à virtualização. Ambas são projetadas para simplificar o código de virtualização e melhorar potencialmente a performance de ambientes totalmente virtualizados.

## **2.6. LINHAS DE DESENVOLVIMENTO – INTEL E AMD**

Sabe-se que a Intel e a AMD vem investindo em tecnologia para permitir a virtualização em processadores de arquitetura x86. As duas tecnologias introduziram arquiteturas similares, implementando um assistente em hardware (conhecido como hardware assist) para suportar virtualização de uma forma nativa, porém as tecnologias das duas fabricantes são incompatíveis entre si. Com esta nova camada na CPU, o monitor de máquinas virtuais tem seu próprio nível privilegiado onde ele executa, e também não é mais necessário que seja retirado o privilégio dos sistemas convidados, uma vez que os sistemas operacionais executam diretamente sobre o hardware.

A Intel deu o nome da versão de seu hardware assist de “VT” (“Virtualization Technology”) que anteriormente era chamado de “Vanderpool”, enquanto a AMD nomeou de “SVM” (“Secure Virtual Machine”) e mais recentemente, acabou mudando para “AMD-V” (“AMD Virtualization”), o codinome inicial era “Pacifica”. A idéia é tornar suas CPU estritamente virtualizáveis, adicionando um modo hipervisor. Algumas instruções sensíveis ainda não geram traps no modo usuário, todavia isto não é uma grande preocupação quando o sistema convidado pode executar em modo supervisor. Existem algumas diferenças entre as

implementações da Intel e AMD, contudo os processadores dotados desta tecnologia basicamente possuem um conjunto de instruções extras chamadas de Extensões de Máquina Virtual (Virtual Machine Extensions - VMX). Por exemplo, no caso do Intel-VT, o VMX traz 10 novas instruções específicas para utilização de máquinas virtuais com o processador, são elas: VMPTRLD, VMPTRST, VMCLEAR, VMREAD, VMWRITE, VMCALL, VMLAUCH, VMRESUME, VMXOFF e VMXON. Para entrar no modo de virtualização, o software deve executar a instrução VMXON e então chamar o monitor de máquinas virtuais. Feito isso, o monitor pode entrar em cada máquina virtual usando a instrução VMLAUNCH, e sair delas usando a instrução VMRESUME. Se o monitor quiser parar todas as máquinas virtuais e sair do modo de virtualização, ela executa a instrução VMXOFF. O SVM disponibiliza a instrução VMRUN para executar uma máquina virtual, VMSAVE e VMLOAD são utilizadas para complementar as capacidades de guardar e restaurar estados da instrução VMRUN e dar acesso ao estado do processador. A instrução VMCALL permite que o sistema operacional se comunique diretamente com o monitor. Em termos de gerenciamento de memória, existe uma diferença relevante entre a tecnologia da AMD e Intel. Nos processadores da AMD o gerenciamento de memória é feito por hardware enquanto que nos processadores da Intel ele é feito por software. Por esta razão, o desempenho da arquitetura SVM pode ser mais elevado que o da arquitetura Intel-VT, embora esta eficiência ainda não tenha sido efetivamente comprovada. Outro avanço dessas tecnologias de virtualização é a inclusão de virtualização de E/S. Atualmente as soluções de virtualização por software não podem exclusivamente determinar que uma máquina virtual acesse diretamente um hardware físico (como uma placa de rede, por exemplo), tendo que simular estas operações com a utilização de técnicas complexas. Desse modo, podemos concluir que a principal vantagem dessas tecnologias da Intel e AMD é uma melhora significativa de desempenho na virtualização de CPU, pois uma vez que há uma camada de virtualização nativa no hardware, não existe a necessidade de tradução binária.

## **2.7. ARMAZENAMENTO**

Dentre os diversos tipos de armazenamento de dados, os mais utilizados pelas empresas são HD externos, fitas DAT, storages, entre outros.

### 2.7.1. HD EXTERNO

Hard Disks externos são dispositivos de armazenamento que são utilizados para guardar dados de forma segura e independente. Geralmente são usados para backup e mantidos fora do ambiente computacional, pois garantem que no caso de perda de dados, como desastres de diversas naturezas, os dados e sistemas possam ser restaurados da maneira mais rápida possível.

### 2.7.2. FITAS DAT

Tem as mesmas funções que o HD externo, porém, com menor espaço para armazenamento de dados. A diferença mais destacada em relação aos HDs externos é a forma como os dados são salvos e consultados, pois diferente dos HDs, as fitas DAT não permitem que os dados sejam localizados de maneira distribuída como nos HDs. A Fita DAT é muito utilizada para backup.

### 2.7.3. STORAGE

Storage é um dispositivo de armazenamento que permite armazenar uma grande quantidade de dados, mantendo assim, um dos ativos mais importantes de uma organização, que são suas informações.

Os storages possuem diversas formas de funcionamento, como nos exemplos:

- HOT SWAP – Possui a capacidade de substituir componentes, como disco de uma máquina sem a necessidade de deixá-la em *downtime*;
- HOT SPARE – O dispositivo está pronto para ser usado em caso de pane, sem intervenção externa. O hardware fica sem uso até ser acionado;
- RAID (*Redundant Array of Independent Disks*) – Trata-se de uma tecnologia que combina vários discos rígidos para formar uma única unidade lógica, onde os mesmos dados são armazenados em todos os discos, de maneira redundante. Esse

procedimento aumenta consideravelmente a segurança dos dados, uma vez que, no caso de um ou mais discos pararem, os outros assumiram as suas funções. O RAID possui 7 níveis, sendo eles o RAID 0, RAID 1, RAID 2, RAID 3, RAID 4, RAID 5 e RAID 0 + 1. Cada um com suas particularidades.

Dentre os tipos de storages, os mais importantes são:

- NAS (*Network Attached Storage*) – É um sistema de armazenamento de dados em ambiente externo que utiliza a rede de dados existentes para comunicação. Seu hardware de armazenamento é anexado a rede.
- DAS (*Direct Attached Network*) - É o armazenamento onde todos os discos e dispositivos estejam no servidor, ao invés de separados. É muito confiável para armazenamento de dados no servidor, possuindo pouca escalabilidade devido a quantidade de discos, onde a alternativa são discos com maiores capacidades.
- SAN (*Storage Area Network*) – Possui hardware dedicado a armazenamento, conexão física feita por fibra ótica, deixando a LAN livre. Utiliza hardware (HBA – *Host Bus Adapter* e switches) e padrão específico (*Fiber Channel*).

### **3. FERRAMENTAS**

#### **3.1. VMWARE**

Dentre todos os softwares de virtualização existentes, o VMware está entre os mais usados. Seu lançamento ocorreu em meados de 1999, tornando-se a primeira solução de virtualização para computadores com arquitetura x86. Sua camada de virtualização suporta diversos sistemas operacionais sobre um hardware.

O VMware é um software proprietário e foi desenvolvido pela empresa VMware Inc., que é subsidiária da EMC Corporation.

Suas principais versões são VMware ESX Server, VMware Server, VMware Workstation e também VMware Player.

##### **3.1.1. VIRTUALIZAÇÃO EM DISCO**

O VMware ESX Server é uma versão comercial do produto destinada ao uso de servidores de grande porte. Trata-se de uma máquina virtual do tipo I, possuindo um sistema operacional próprio e otimizado, com isso, sua principal função é gerenciar máquinas virtuais.

No VMware ESX Server, cada máquina virtual representa um sistema complexo e completo, com processador, memória, disco e BIOS, o que permite um completo ambiente de execução, fazendo com que sistemas operacionais convidados não precisem ser modificados.

O ESX Server implementa seu próprio sistema de arquivos, que é chamado de VMFS. Esse sistema de arquivos é um sistema distribuído que permite que múltiplos hosts tenham acesso à arquivos correspondentes no mesmo volume VMFS. A principal vantagem é que o VMFS é otimizado para operações de E/S com arquivos grandes, como no caso dos arquivos que contém as imagens de máquinas virtuais.

##### **3.1.2. VIRTUALIZAÇÃO DA MEMÓRIA**

Já o ESX virtualiza a memória das máquinas virtuais por meio de tradução de endereços, o monitor realiza um mapeamento da página de memória do sistema operacional convidado para a página de memória física, que fica na subcamada do hardware. Esse processo diz respeito à virtualização da memória, por isso, o ESX mapeia a página da máquina virtual em uma tabela da página sombra (*Shadow Page Table – SPT*) que é atualizado com o da máquina física.

Quando o sistema operacional convidado estabelece um mapeamento novo em sua tabela de página, o monitor detecta a modificação e atualiza a respectiva entrada na tabela de página sombra, que aponta para a localização real da página de memória no hardware. Quando a máquina virtual está executando, o hardware usa diretamente a tabela de página sombra para a tradução do endereço, o que permite que os acessos de memória normais na máquina virtual executem sem adicionar overhead de traduções de endereços, uma vez que as tabelas de página da sombra já estão definidas.

### **3.1.3. VIRTUALIZAÇÃO DE REDE**

No ESX Server é possível definir até quatro adaptadores de rede virtual. Cada adaptador tem seu próprio endereço MAC e endereço IP. As interfaces de rede virtual das múltiplas máquinas virtuais podem ser conectadas a um switch virtual. Cada switch pode ser configurado sem qualquer conexão ou a uma LAN física por meio dos adaptadores de rede da máquina anfitriã. Esses switches são chamados de “VMnets” e são abstrações que garantem conexões com alta velocidade entre as máquinas virtuais, o sistema anfitrião e a LAN física.

### **3.1.4. VMWARE SERVER**

O VMware Server, que anteriormente eram chamado de VMware GSX Server, é a versão para uso em servidores de pequenos e médios portes. Passou a ser gratuito em 2006 e disponibilizado para download no site oficial do fabricante.

O VMware Server é uma máquina virtual do tipo II, onde é necessário que o software execute sobre um sistema operacional anfitrião que pode ser em sistemas operacionais baseados em Linux ou Windows (existe uma versão para cada um destas plataformas).

O programa permite que sejam criadas diversas máquinas virtuais suportando alguns sistemas convidados de uma maneira otimizada, como algumas versões do Windows, Linux, Solaris e BSD. Existe também um modo genérico para se utilizar outros sistemas operacionais sem suporte específico.

O VMware Server, assim como o VMware ESX, também suporta máquinas virtuais com uma ou duas CPU virtuais.

Ele pode compartilhar com os sistemas convidados, periféricos do hardware como: CDROM, placas de rede e portas USB.

Com ele existe a possibilidade de criar registros instantâneos (chamado de "snapshot") de uma máquina virtual num dado momento, no qual é possível fazer backup em um determinado estado, ou testar configurações em que se pode reverter.

#### **3.1.5. VMWARE WORKSTATION**

Trata-se também de uma versão comercial do VMware, sendo utilizada em estações de trabalho. Possui basicamente os mesmos recursos do VMware Server, inclusive com a possibilidade de criar máquinas virtuais. O VMware Workstation destaca-se pela facilidade de uso proporcionada por seus assistentes que guiam o usuário no processo de criação de máquinas virtuais. Ele também possui um assistente que ajuda a montar clones de máquinas virtuais. Também é possível criar grupos de máquinas virtuais, de uma só vez, e colocá-las em redes. Com o VMware Workstation é possível criar máquinas virtuais em dispositivos externo como um disco rígido ou um pen-drive, através de um produto adicional chamado ACE Option Pack.

#### **3.1.6. VMWARE PLAYER**

O VMware Player trata-se da versão mais simples do produto e que também é disponibilizada gratuitamente para download. O VMware Player é indicado para aplicações leves e não pode criar máquinas virtuais, porém executa as máquinas virtuais criadas por outras versões mais completas.

#### **3.1.7. VMWARE HA (HIGH AVAILABILITY)**



O VMware HA proporciona a alta disponibilidade na infra-estrutura virtual dos ambientes de TI sem o custo e a complexidade das soluções de cluster. O VMware HA é uma funcionalidade que, integrada ao VirtualCenter, faz a monitoração contínua de todos os servidores físicos e, em caso de falha de um destes, reinicia as máquinas virtuais afetadas em um outro servidor.

#### **3.1.7.1. SEGURANÇA CONTRA FALHAS**

Com o VMware HA é possível proteger aplicativos sem a necessidade de outra opção de failover, fornecendo alta disponibilidade de forma econômica a qualquer aplicativo executado em uma máquina virtual. As soluções de alta disponibilidade geralmente são complexas e caras, ficando mais voltadas a aplicativos que atuam em situações críticas. O VMware HA proporciona uma solução de alta disponibilidade e sem um alto custo, permitindo desta forma estendê-la a aplicativos de software que não tinham essa condição.

Diferente de outras soluções de alta disponibilidade mais específicas de sistemas operacionais ou aplicativos, o VMware HA pode ser considerado uma opção de solução consistente e de fácil gerenciamento, provendo alta disponibilidade para todo um ambiente de TI. Desta maneira, o VMware HA permite o failover básico de qualquer aplicativo, com custos e despesas gerais de gerenciamento mínimo.

#### **3.1.7.2. FUNCIONAMENTO**

A função do VMware HA é monitorar de maneira contínua todos os servidores em um pool de recursos e detectar possíveis falhas de servidor. Cada servidor possui um agente, onde esse agente mantém um *heartbeat*, (núcleo do ambiente de alta disponibilidade) com outros servidores no pool de recursos, e uma perda de *heartbeat* ocasiona o processo de reinicialização de todas as máquinas virtuais afetadas em outros servidores. O VMware HA permite que haja sempre recursos suficientes disponíveis no pool de recursos, podendo reinicializar as máquinas virtuais em outros servidores físicos em caso de falha do servidor. Assim, a reinicialização das

máquinas virtuais é possibilitada pelo sistema de arquivos em cluster do Virtual Machine File System (VMFS), que fornece a diversas instâncias do ESX Server acesso simultâneo de leitura e gravação aos mesmos arquivos de máquinas virtuais. O VMware HA é configurado de maneira fácil para um pool de recursos com o VirtualCenter.

### **3.1.7.3. PRINCIPAIS RECURSOS**

### **3.1.7.4. DETECÇÃO AUTOMÁTICA DE FALHAS DE SERVIDOR**

É possível automatizar o monitoramento da disponibilidade dos servidores físicos, pois o VMware HA detecta falhas de servidor e aciona a reinicialização das máquinas virtuais sem qualquer intervenção humana.

### **3.1.7.5. VERIFICAÇÃO DE RECURSOS**

O VMware HA garante que haja sempre capacidade disponível para reiniciar todas as máquinas virtuais afetadas por uma falha de servidor, monitorando de maneira contínua a utilização da capacidade e a reserva de capacidade extra, de forma que seja possível a reinicialização das máquinas virtuais.

### **3.1.7.6. REINICIALIZAÇÃO AUTOMÁTICA DE MÁQUINAS VIRTUAIS**

Com a reinicialização automática é possível proteger qualquer aplicativo em outro servidor físico do pool de recursos.

### **3.1.7.7. ESCOLHA INTELIGENTES DE SERVIDORES**

Quando utilizado com o VMware Distributed Resource Scheduler (DRS), o VMware HA propicia uma automação ideal das máquinas virtuais reinicializadas após uma falha de servidor.

### 3.1.7.8. VANTAGENS

Minimizar o tempo de inatividade e a interrupção dos serviços de TI, eliminando também a necessidade de hardware dedicado em standby e instalação de software adicional. O VMware HA fornece alta disponibilidade uniforme em todo o ambiente virtualizado, sem o alto custo ou a complexidade das soluções de failover associadas a sistemas operacionais ou aplicativos específicos.

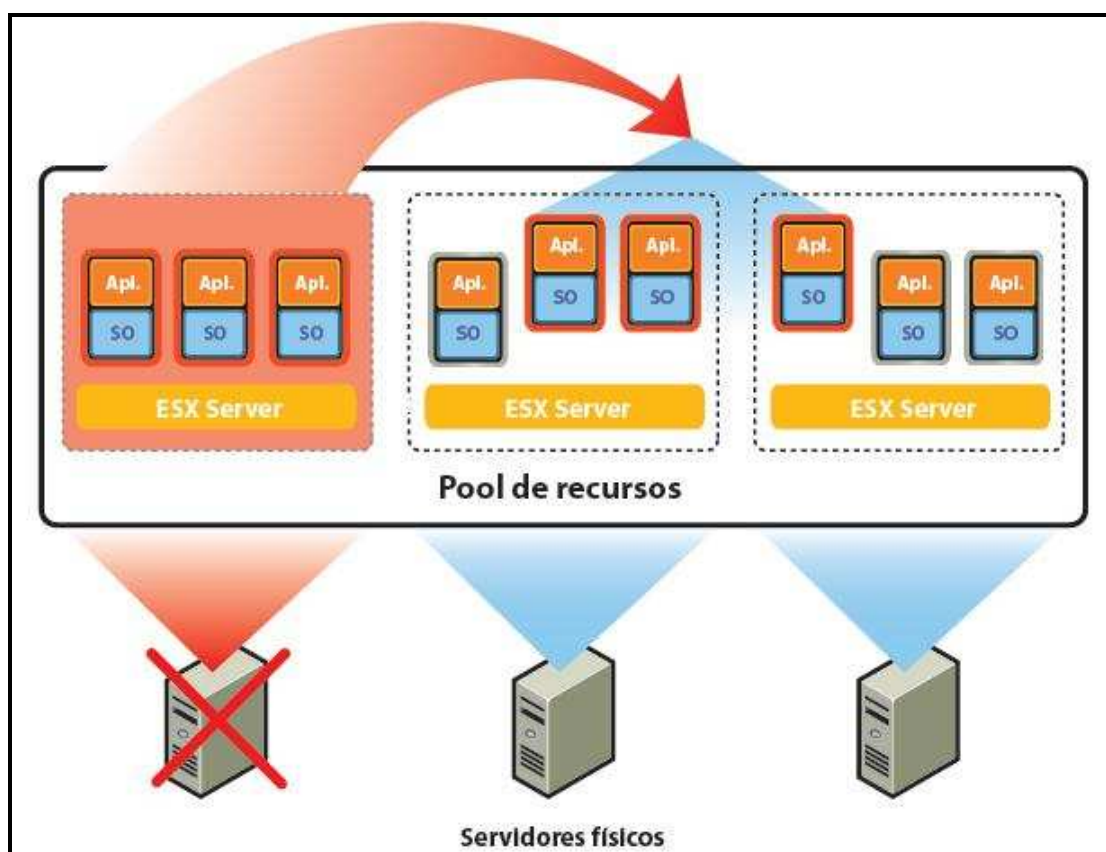


Figura 4. Representação da estrutura do VMware HÁ  
Fonte: VMware Infrastructure

### 3.1.8. VMWARE DRS (DISTRIBUTED RESOURCE SCHEDULER)

A função do VMware DRS é alocar e equilibrar dinamicamente a capacidade computacional entre um conjunto de recursos de hardware agregados em um pool lógico de recursos. Dessa maneira, o VMware DRS realiza o monitoramento de forma contínua da utilização dos pool de recursos e aloca os recursos disponíveis de forma inteligente entre as máquinas virtuais, baseando-se em regras predefinidas, assim refletindo as necessidades dos negócios e as mudanças de prioridade. Quando há um aumento de carga em uma máquina virtual, o VMware DRS aloca recursos adicionais automaticamente, redistribuindo as máquinas virtuais entre os recursos físicos no pool de recursos.

O VMware DRS pode ser configurado para funcionar de maneira automática ou manual. Na forma automática o DRS determina a melhor distribuição possível das máquinas virtuais entre diversos servidores físicos e realiza automaticamente sua migração para os servidores físicos mais adequados. Já o VMware DRS configurado no modo manual fornece uma recomendação para o posicionamento ideal das máquinas virtuais, deixando ao administrador do sistema a decisão de realizar ou não a alteração.

A organização hierárquica flexível de pools de recursos permite aos administradores adequar recursos de TI disponíveis às necessidades da organização de negócios. As unidades individuais de negócios podem receber recursos dedicados de TI, beneficiando-se, ao mesmo tempo, da eficiência dos pools de recursos. Os privilégios eficientes de acesso tornam possível delegar tarefas rotineiras de infra-estruturas do pool de recursos de uma unidade de negócios ao administrador da unidade de negócios.

#### **3.1.8.1. ALINHAMENTOS DE RECURSOS**

É possível definir regras e políticas para decidir como os recursos deverão ser priorizados entre as máquinas virtuais, assim o VMware DRS aloca dinamicamente e de forma inteligente os recursos de TI para as máquinas virtuais de maior prioridade, proporcionando o alinhamento ideal entre os negócios de TI.

#### **3.1.8.2. AUTONOMIA DE TI**

Pode-se criar uma infra-estrutura dedicada de TI, destinadas às unidades de negócios, buscando o maior aproveitamento dos recursos e ao mesmo tempo, uma maior utilização de hardware obtida com os pools de recursos.

#### **3.1.8.3. AUMENTO DA PRODUTIVIDADE DOS ADMINISTRADORES DE SISTEMAS**

O VMware DRS permite que só um administrador de sistemas monitore e gerencie com eficiência um amplo pool de recursos de infra-estrutura.

#### **3.1.8.4 MANUTENÇÃO DE HARDWARE**

Coloca um servidor físico em modo de manutenção e o VMware DRS migrará automaticamente todas as máquinas virtuais para outros servidores físicos, possibilitando a manutenção do servidor sem tempo de inatividade.

#### **3.1.8.5 CAPACIDADE ADICIONAL**

Permite o adicionamento de novos servidores físicos a um pool de recursos, assim o VMware DRS aproveitará automaticamente a capacidade adicional, redistribuindo as máquinas virtuais entre os servidores.

#### **3.1.8.6 POOL DE RECURSOS**

O VMware DRS agrega recursos distintos de hardware em pools lógicos unificados de recursos. Desta maneira, os pools de recursos são otimizados de uma forma automática e inteligente, garantindo que a alocação dos recursos de TI corresponda às prioridades de negócios e maximize a utilização de hardware.

### **3.1.8.7. ABSTRAÇÃO DE RECURSOS DE HARDWARE**

É possível gerenciar os recursos de hardware independentemente dos servidores físicos que os contenham.

### **3.1.8.8. HIERARQUIA FLEXIVEL**

Com o VMware DRS é possível organizar os pools de recursos de uma forma hierárquica para a adequação dos recursos de TI disponíveis à organização de negócios. O DRS possibilita a máxima utilização dos recursos. Ao mesmo tempo que as unidades de negócios mantêm o controle da autonomia de sua infra-estrutura. Os pools de recursos podem ser adicionados, removidos ou reorganizados de forma flexível conforme as necessidades de negócios ou que as empresas se modificam.

### **3.1.8.9. ISOLAMENTO ENTRE POOL DE RECURSOS**

Permite mudanças de alocação em um pool de recursos sem afetar outros pool de recursos não-relacionados. Como exemplo, qualquer mudança de alocação no pool dedicado a uma determinada unidade de negócios não tem efeito sobre outros pools de recursos.

### **3.1.8.10. CONTROLE DE ACESSO E DELEGAÇÃO**

Garante alocação de recursos em vários níveis da empresa, eliminando os gargalos. A criação e a manutenção das máquinas virtuais para uma unidade de negócios pode ser delegada ao administrador do sistema da unidade, eliminando a dependência organizacional central de TI para todas as operações de rotinas.

### **3.1.8.11. GERENCIAMENTO DE CONJUNTOS DE MÁQUINAS VIRTUAIS**

O VMware DRS otimiza o nível de serviço de aplicativos distribuídos, efetuando um controle da alocação agregada de recursos para todo o conjunto de máquinas virtuais, executando o aplicativo distribuído.

#### **3.1.8.12. MODOS MANUAL E AUTOMÁTICO**

As informações sobre a utilização de recursos por servidores e máquinas virtuais são coletadas pelo VMware DRS e em seguida gera recomendações para otimizar a alocação das máquinas virtuais. Tais recomendações podem ser executadas de modo automático ou manual.

#### **3.1.8.13. POSICIONAMENTO INICIAL**

Quando uma máquina virtual é ativada pela primeira vez, o VMware DRS a posiciona automaticamente no servidor físico mais adequado ou faz alguma recomendação.

#### **3.1.8.14. OTIMIZAÇÃO CONTÍNUA**

Otimiza continuamente a alocação de recursos, com base nas regras definidas para isso e na utilização de recursos. Essas mudanças na alocação de recursos podem ser executadas automaticamente, com a migração em tempo real das máquinas virtuais utilizando o VMotion. Caso seja optado, o modo manual do VMware DRS fornece recomendações de execução aos administradores do sistema.

#### **3.1.8.15. MODO DE MANUTENÇÃO PARA OS SERVIDORES**

O VMware DRS realiza manutenção dos servidores físicos sem a necessidade de interrupção dos serviços para as máquinas virtuais e os usuários finais. Quando um servidor físico é colocado em modo de manutenção, o VMware DRS faz a identificação de servidores

alternativos nos quais as máquinas virtuais podem ser executadas. Baseando-se nas configurações do modo de automação, as máquinas virtuais são movidas automaticamente para os servidores alternativos, ou então o administrador do sistema realiza a movimentação manualmente, seguindo as orientações do VMware DRS.

#### **3.1.8.16. REGRAS DE AFINIDADES**

O VMware DRS permite a criação de regras para o controle da alocação das máquinas virtuais nos servidores físicos. Por exemplo, certas máquinas virtuais podem ser sempre executadas no mesmo servidor por questão de desempenho. Entretanto, determinadas máquinas virtuais podem ser sempre executadas em servidores diferentes para maior disponibilidade.

#### **3.1.8.17. VANTAGENS**

Priorizar recursos para os aplicativos de maior valor, de forma a alinhar os recursos às metas de negócios.

Otimizar a utilização de hardware de forma automática e contínua, respondendo às mudanças constantes das condições.

Fornecer uma infra-estrutura dedicada (virtual) às unidades de negócios, proporcionando, ao mesmo tempo, à TI controle total sobre o hardware.

Realiza a manutenção de servidores sem tempo de inatividade.



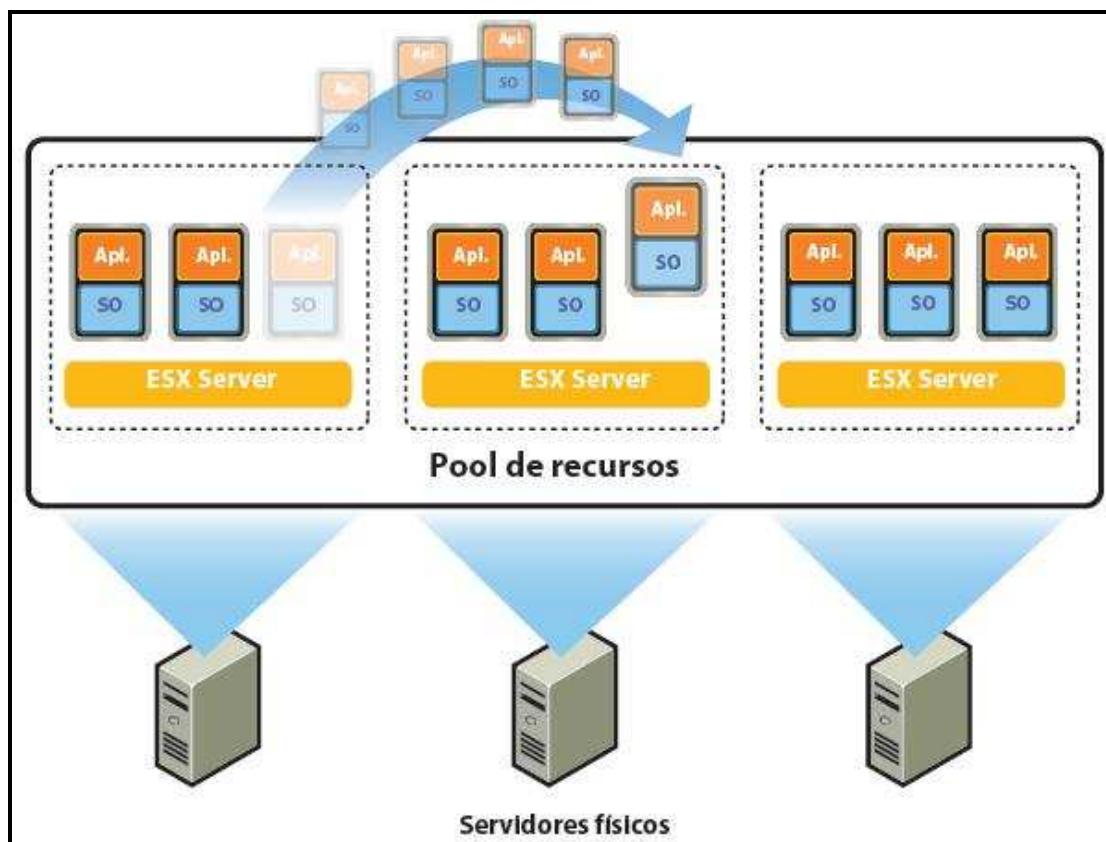


Figura 5. Representação da estrutura do VMware DRS  
 Fonte: VMware Infrastructure

### 3.1.9. VMWARE VMOTION

O VMware VMotion permite a migração em tempo real de máquinas virtuais em execução de um servidor físico para outro, sem tempo de inatividade, mantendo a disponibilidade contínua de serviços e a total integridade de transações. O VMware VMotion é uma tecnologia essencial para viabilizar a criação de um Data Center dinâmico, automatizado e auto-otimizado.

#### 3.1.9.1. UTILIZAÇÃO DO VMWARE VMOTION

Permite que os usuários otimizem e aloquem automaticamente pools inteiros de recursos, possibilitando a utilização de hardware, garantindo flexibilidade e a máxima disponibilidade.

Realiza a manutenção de hardware sem tempo de inatividade programado.

Realiza a migração de máquinas virtuais de maneira proativa, retirando-as de servidores com falhas ou apresentando baixo desempenho.

### **3.1.9.2. FUNCIONAMENTO DO VMWARE VMOTION**

A realização da migração em tempo real de uma máquina virtual de um servidor físico para outro com o VMware VMotion é possibilitada por três tecnologias subjacentes.

Primeiramente, todo o estado de uma máquina virtual é encapsulado por um conjunto de arquivos armazenados em uma storage compartilhada como Fibre Channel, SAN (Storage Area Network, rede de armazenamento de dados) iSCSI ou NAS (Network Attached Storage, armazenamento conectado à rede). O VMware Virtual Machine File System (VMFS) em cluster permite que várias instalações do ESX Server acessem simultaneamente os mesmos arquivos em uma máquina virtual.

Segundo, a memória ativa e o estado preciso de execução da máquina virtual são transferidos rapidamente por uma rede de alta velocidade, possibilitando que a máquina virtual transfira instantaneamente sua execução do ESX Server de destino. O VMotion mantém o período de transferência imperceptível para os usuários, fazendo com que o controle das transações contínuas de memória em um bitmap sejam mantidas. Assim, quando toda a memória e o estado do sistema tiverem sido copiados para o ESX Server de destino, o VMotion suspende a máquina virtual de origem, faz uma cópia do bitmap para o ESX Server de destino e reinicia a máquina virtual no ESX Server de destino. Todo esse processo leva menos de dois segundos em uma rede Gigabit Ethernet.

Terceiro, as redes de uso pela máquina virtual também são virtualizadas pelo ESX Server subjacente, garantindo que mesmo após a migração, a identidade e as conexões de rede da máquina virtual sejam preservadas. O VMotion gerencia o endereço MAC virtual como parte do processo. Quando a máquina de destino é ativada, o VMotion notifica o roteador da rede, para garantir o reconhecimento da nova localização física do endereço MAC virtual. Uma vez que a migração de uma máquina virtual com o VMotion preserva o estado preciso de execução, a

identidade e as conexões ativas de rede, o resultado é tempo de inatividade zero e nenhuma interrupção para os usuários.

#### **3.1.9.3. CONFIABILIDADE**

Segundo o fabricante, “Comprovado por milhares de clientes em ambientes de produção desde 2004, o VMotion continua definindo o padrão para os mais confiáveis recursos de migração em tempo real” [VMware]

#### **3.1.9.4. DESEMPENHO**

Possibilita a realização de migração em tempo real, com tempo de inatividade imperceptível para os usuários finais. O uso da CPU e dos recursos de rede garante que as migrações em tempo real ocorram com rapidez e eficiência.

#### **3.1.9.5. INTEROPERABILIDADE**

Permite migrar máquinas virtuais executando qualquer sistema operacional, em qualquer tipo de hardware e de storage compatível com o VMware ESX Server.

#### **3.1.9.6. CAPACIDADE DE GERENCIAMENTO**

Permite a rápida identificação do melhor destino para uma máquina virtual, fazendo uso de informações em tempo real, fornecidas pelo assistente de migração.

Possibilita que sejam realizadas várias migrações simultâneas para otimizar continuamente o posicionamento das máquinas virtuais em todo o ambiente de TI.

O VMotion permite atribuir prioridades a cada operação de migração em tempo real, garantindo que as máquinas virtuais mais importantes tenham sempre acesso aos recursos de que precisam.

É possível automatizar tarefas programadas de migração para que ocorram em horários predefinidos e sem a presença de um administrador.

Pode-se manter um registro detalhado das operações de migração, incluindo a data e hora e os administradores responsáveis por iniciá-las.

### 3.1.9.7. VANTAGENS

Possibilita alocar máquinas virtuais de forma contínua e automática nos pools de recursos.

Melhora a disponibilidade, realizando a manutenção sem a interrupção das operações de negócios.

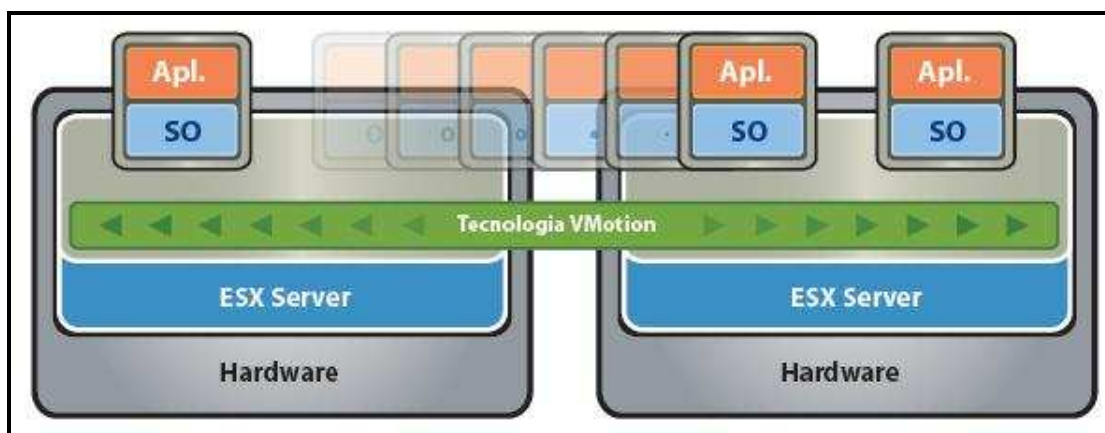


Figura 6. Representação da estrutura do VMware VMotion  
Fonte: VMware Infrastructure

### 3.1.10. VMWARE VCB – CONSOLIDATED BACKUP

O VMware VCB possibilita o backup de máquinas virtuais de forma centralizada. O VMware VCB suporta o backup através da rede SAN, o que reduz de maneira significativa o

tempo de backup e, além disso, proporciona o backup de máquinas virtuais em execução, possibilitando assim, a continuidade dos serviços

O VMware *Consolidated Backup* permite que seja feito o backup das máquinas virtuais a qualquer momento em instalações de virtualização baseadas em VMware utilizando um proxy server que não requeira muito processamento dos hosts.

O uso do VCB permite que os ciclos do CPU dos hosts utilizando um servidor proxy tenham menor perda de tempo para a realização de backup.

Com o VCB é possível reduzir o overhead com a centralização do gerenciamento dos backups das Máquinas virtuais.

Pelo fato de usar a tecnologia de snapshot do VMFS, o VCB possibilita que as máquinas virtuais continuem em execução durante a realização do backup.

#### **3.1.10.1. TIPOS DE BACKUPS**

O VCB utiliza dois tipos de backups, Full-Image Backup e File-Level Backup.

##### **Full-Image Backup**

Com o uso do VCB e o backup client, é possível fazer o backup full de qualquer outra máquina virtual independente do sistema operacional convidado.

##### **File-Level Backup**

Fazendo o uso do VCB em conjunto com o backup client, pode-se fazer o backup a nível de arquivo de máquina virtual executando windows permitindo assim, um backup a nível de diretório e arquivo. Dessa maneira, é possível criar uma política de backup incremental, diferencial e full para os arquivos e diretórios.

### **3.1.10.2. REQUISITOS NECESSÁRIOS**

Para instalações baseadas em SAN FC “*Storage Area Network Fiber Channel*” é necessário que se tenha um servidor físico para o backup proxy server executando ao menos o Windows Server 2003 R2 ou o Windows Server 2003 Service Pack 1. Esse servidor deverá utilizar HBAs FC “*Host Bus Adapter Fiber Channel*” para se conectar ao storage. É importante que as máquinas virtuais sejam armazenadas em um datastore VMFS 3 no storage. Assim, o VMFS irá armazenar as imagens.

Para a utilização do RDM “*Raw Device Mapped*”, outro sistema de arquivos na SAN, é necessário o uso do virtual *compatibility mode*.

O aconselhável é que o backup proxy seja também o backup media server para o software de backup e que se compatibilize com a versão do software de backup de 32 ou 64 bits com a versão do Windows de 32 ou 64 bits.

### **3.1.10.3. VERSÃO**

A versão 3.5 do VMware VI geralmente é utilizada devido a compatibilidade com o storage, mas com a versão 4.1, o VCB ganhou novas opções:

Sua utilização pode ser assumida em redes iSCSI (software ou hardware iniciador) e NAS e em disco local.

Os snapshots podem ser removidos pela LAN também e não apenas pela SAN.

O proxy server pode ser uma máquina virtual, pois em iSCSI o iniciador, que é o software cliente, precisa ser por software, onde rodava sobre o Windows Server 2003.

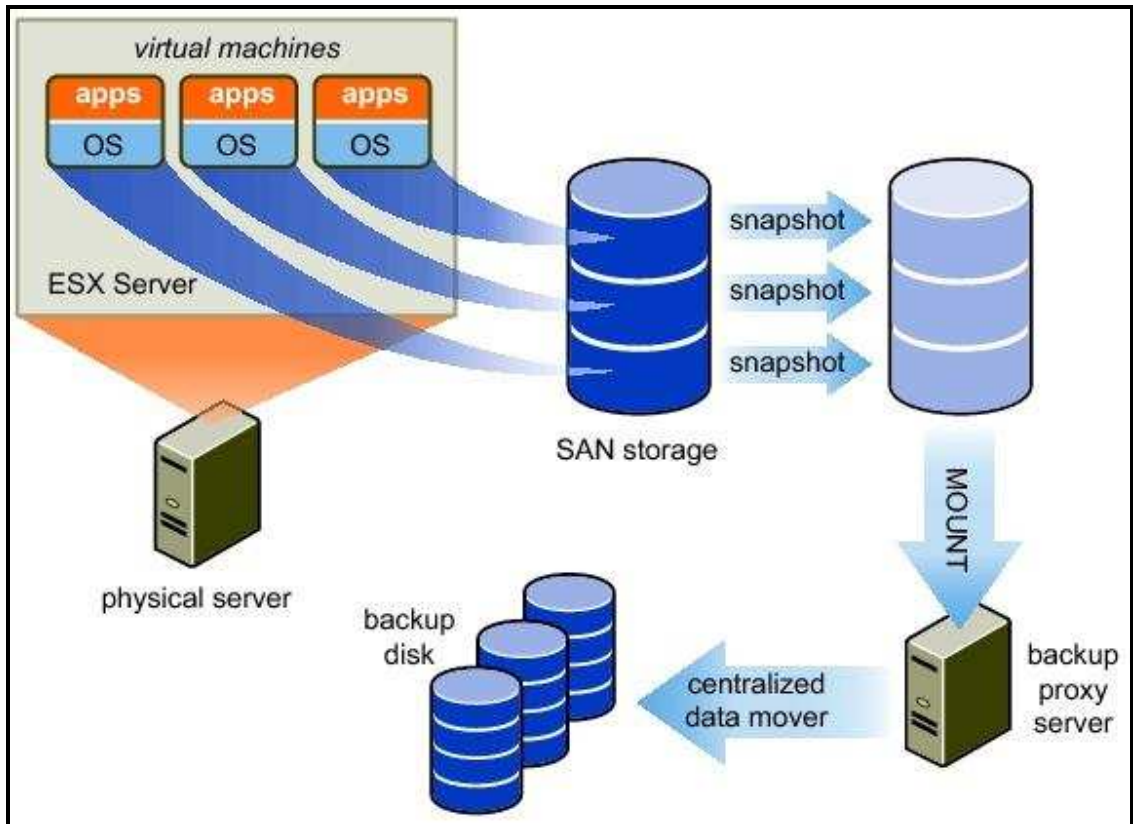


Figura 7. Estrutura do VMware Consolidated Backup.

Fonte: VMware Infrastructure

### 3.1.11. VMWARE vSTORAGE VMFS

O VMware vStorage *Virtual Machine File System* (VMFS) é um sistema de arquivos de cluster de alto desempenho que fornece virtualização de armazenamento otimizado para máquinas virtuais. Cada máquina virtual é encapsulada em um pequeno conjunto de arquivos e o VMFS é o sistema de armazenamento padrão para esses arquivos nos discos e nas partições SCSI físicos.

O VMFS permite que diversas instâncias do VMware ESX acessem o armazenamento da mesma máquina virtual e, como resultado, as máquinas virtuais podem ser migradas de forma dinâmica e automática entre instâncias do VMware ESX.

Sem o uso do vStorage não seria possível utilizar ferramentas como o VMware HA, VMware DRS e o VMware vMotion, além de outras ferramentas.

O VMware vMotion, por exemplo, quando irá realizar a migração de uma máquina virtual de um servidor físico que acaba de perder seus serviços para outro servidor ativo, busca os dados já salvos no storage, permitindo assim que o servidor volte ao funcionamento em curto prazo de tempo, muitas vezes passando despercebido pelo usuário.

#### **3.1.11.1. UTILIZAÇÃO**

O VMware vStorage VMFS é um pré-requisito para o desenvolvimento de um data center dinâmico, automatizado e auto-otimizado. O VMFS possibilita que serviços sejam distribuídos com base na virtualização, como:

- Otimização de recursos distribuídos – O VMFS permite que diversas instancias do VMware ESX acessem o armazenamento da mesma máquina virtual e, como resultado, as máquinas virtuais podem ser migradas de forma dinâmica e automática entre instancias do VMware ESX, viabilizando:
  - A alocação dinâmica de recursos em pools de recursos;
  - A migração em tempo real das máquinas virtuais em execução entre servidores distintos.
- Alta disponibilidade – O VMFS gerencia bloqueios em discos e reservas de SCSI, permitindo:
  - O cluster de máquinas virtuais com o Microsoft Clustering Services;
  - A reinicialização automática das máquinas virtuais em servidores físicos distintos.



- Backup eficiente fora do host – O VMFS permite que um serviço de Proxy faça backup no snapshot de uma máquina virtual enquanto a máquina virtual realiza leituras/gravações em seu sistema de armazenamento.

### **3.1.11.2. FUNCIONAMENTO DO VMFS**

O VMFS foi otimizado e rigorosamente testado e certificado para uma grande variedade de equipamentos Fiber Channel e SAN iSCSI. O VMFS armazena com eficiência todo o estado da máquina virtual em um local central e pode ser criado com antecedência, permitindo o provisionamento instantâneo de máquinas virtuais sem depender de um administrador de armazenamento.

Os sistemas de arquivos convencionais permitem que somente um servidor tenha acesso de leitura/gravação ao mesmo arquivo por vez. A contrário disso, o VMFS é um sistema de arquivos de cluster que aproveita o armazenamento compartilhado para permitir varias instancias do VMware ESX acesso simultâneo de leitura/gravação ao mesmo sistema de armazenamento. O VMFS fornece bloqueio em disco para garantir que uma máquina virtual não seja inicializada por varias instalações do VMware ESX ao mesmo tempo. Caso um servidor venha falhar, o bloqueio em disco de cada máquina virtual é liberado, permitindo que a máquina virtual seja reinicializada em outros servidores físicos.

### **3.1.11.3. PRINCIPAIS RECURSOS**

Sistema de arquivos em cluster – Possibilita que seja criado a base para os serviços de infra-estrutura distribuída baseados na virtualização, armazenando os arquivos das máquinas virtuais em um sistema de armazenamento compartilhado, como Fiber Channel e SAN iSCSI.

Sistema de arquivos com dados compartilhados – Permite que várias instalações do VMware ESX leiam e gravem simultaneamente no mesmo local de armazenamento.

Inserção ou exclusão de nós on-line – O VMFS possibilita que seja adicionado ou excluído um host do VMware ESX e de um volume VMFS sem pausar ou interromper o processamento de outros hosts do ESX no mesmo volume.

Bloqueio de arquivos em disco – Evita que as máquinas virtuais sejam inicializadas por vários servidores ao mesmo tempo.

#### **3.1.11.4. VANTAGENS**

O VMFS possui uma simplificação considerável do provisionamento e da administração de máquinas virtuais, armazenando com eficiência todo o estado da máquina virtual em um local central.

Permite a execução de várias instâncias do VMware ESX para acessar simultaneamente o sistema de armazenamento da mesma máquina virtual.

Possui suporte de serviços de infra-estrutura distribuída baseados na virtualização, utilizado VMware vCenter Server, VMware vMotion, VMware DRS e VMware HA.

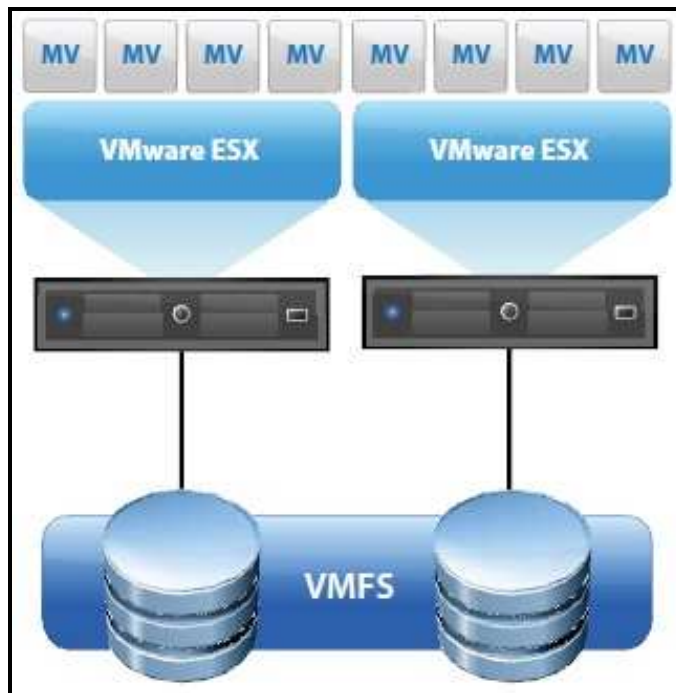


Figura 8. Estrutura do VMware vStorage VMFS

Fonte: VMware Infrastructure

### 3.1.12. LINHA DE COMANDO

Os produtos da VMware não são acessados apenas com interface gráfica, mas também com linhas de comando.

Devido ao fato do kernel das máquinas virtuais da VMware serem baseados no Red Hat Linux, muitos comandos Linux podem ser utilizados na VMware. Além dos comandos Linux, existem também alguns comandos específicos.

Para acessar o modo linha de comando na VMware, pode-se utilizar diversos aplicativos, como o Putty (SSH), por exemplo.

Existem diversos comandos importantes que permitem um gerenciamento da VMware, inclusive remotamente.

Alguns desses comandos estão listados abaixo:

Comandos

Find – procura e mostra arquivos;

Cat – mostra o conteúdo do arquivo;

Grep – procura por partes específicas de um texto num arquivo;

Service – Pode iniciar, parar ou reestartar um serviço;

Nano and vi – Editor de texto simples e fácil de usar;

Su - comando para controlar as contas;

Sudo – Executa comandos com outro usuário, conforme especificado em arquivos de configuração;

Vmkping – É a versão do comando ping. Usa o IP do kernel da vm e executa o ping de outro host ESX;

Esxtop – Soluciona problemas de desempenho. Também fornece em tempo real o histórico das estatísticas de desempenho da CPU, memória, disco e uso da rede;

Vmware-cmd – É um comando versátil para o gerenciamento e recuperação de informações de máquinas virtuais. Pode também mudar os estados de energia, gerenciar, cancelar vms, recuperar e definir informações;

Esxcfg firewall – Esse comando exibe informações e configura o firewall que protege o serviço. Permite e bloqueia portas TCP.

### 3.1.13. SUPORTE VIA SSH

Diante de todo o cuidado com segurança que se deve ter com a infra-estrutura e principalmente seus servidores, é raro encontrar algum servidor VMware diretamente exposto na internet.

E alguns casos, os acessos remotos aos servidores são realizados através de VPN (*Virtual Private Network*), ou até mesmo algum software de acesso remoto desktop, mas umas das maneiras mais práticas e seguras para acesso remoto em servidores são o SSH (*Secure Shell*).

Assim que o acesso através do SSH em um sistema dentro da rede estiver disponível, torna-se uma tarefa um tanto quanto simples criar túneis virtuais para os servidores VMWare. Esta é uma forma segura de gerenciar os dispositivos, porque todo o tráfego passa por uma espécie de túnel criptografado e além do próprio serviço SSH, o usuário não estará interagindo com outros serviços internos.

Para que seja possível ter acesso remoto ao VMware servidor, são necessários dois túneis SSH, um HTTPS túnel (normalmente porta 443) e um túnel console (normalmente porta 902).

Abaixo, encontra-se o exemplo de um script que pode ser usado para criar túneis a partir de qualquer distribuição Linux, OSX ou qualquer outro sistema operacional UNIX.

```
#!/bin/sh
# Ip local. Endereço para extremidade do túnel
LOCAL_IP=192.168.1.1
# Conexão SSH detalhada
SSH_USER=sshuser
SSH_HOST=ssh.host.com
SSH_PORT=62222

# Configuração do servidor VMWare
VMWARE_IP=$2
VMWARE_WEB_PORT=443
VMWARE_CONSOLE_PORT=902
echo "Gerenciando VMWare server at $VMWARE_IP"
echo "Acessando via $LOCAL_IP:$VMWARE_WEB_PORT"
echo "Pressione CTRL+C para encerrar"
case "$1" in
console)
sudo ssh -N -L
$LOCAL_IP:$VMWARE_CONSOLE_PORT:$VMWARE_IP:$VMWARE_CONSOLE_PORT
$SSH_USER@$SSH_HOST -p $SSH_PORT
;;
web)
sudo ssh -N -L $LOCAL_IP:$VMWARE_WEB_PORT:$VMWARE_IP:$VMWARE_WEB_PORT
$SSH_USER@$SSH_HOST -p $SSH_PORT
;;
esac
```

As configurações necessárias:

No início do arquivo é necessário editar o LOCAL\_IP, SSH\_USER, SSH\_HOST e SSH\_PORT, variáveis específicas para atender a sua configuração.

LOCAL\_IP - Geralmente o desktop, endereço IP (ou 127.0.0.1);

SSH\_USER - Conta de usuário para acessar com SSH;

SSH\_HOST - O nome de host com o serviço SSH acessível;

SSH\_PORT - A porta que o SSH está sendo executado.

Por questões de segurança o SSH deve ser executado em uma porta diferente do padrão (ou seja, não 22).

Para que esse script inicie sua função, é preciso deixá-lo como um arquivo executável. Para isso, basta digitar o seguinte comando:

```
# chmod a+x vmware-manage.sh
```

Para gerenciar o VMware como um servidor interno IP 10.1.1.5 , o comando será:

```
# ./vmware-manage.sh web 10.1.1.5
```

Será solicitado uma senha local (para acesso do sudo) e uma senha do SSH.

Uma vez criado, deverá ser aberto um segundo console (terminal) e criar o segundo túnel de acesso:

```
# ./vmware-manage.sh console 10.1.1.5
```

Será possível acessar seu servidor VMWare em <https://192.168.1.1> (ou seja, o endereço LOCAL\_IP endereço).

Esses túneis deverão ser inutilizados com a seguinte ação: Pressionar as teclas CTRL + C ao mesmo tempo.

### **3.2. VIRTUAL BOX**

O VirtualBox é um software de virtualização para arquitetura x86, que foi desenvolvido pela empresa Innotek GmbH, com sede na Alemanha. Desde janeiro de 2007 possui uma versão

open source de licença GNU GPL. O software é uma máquina virtual do tipo II e executa como um processo de sistema operacional host que pode ser Linux, Windows 32 ou 64 bits, ou Mac OS X.

Hoje a empresa SUN Microsystems, proprietária do VirtualBox, é de propriedade da ORACLE Corporation. Aquisição aconteceu no início do ano de 2009.

Atualmente o VirtualBox suporta sistemas convidados como DOS, FreeBSD, Linux, OpenBSD, NetBSD, Solaris, Netware, OS/2 Warp e Windows. Ele utiliza a técnica da virtualização total, emulando componentes chaves do hardware. Com isso, não há necessidade de que os sistemas operacionais convidados sejam modificados para que executem em uma máquina virtual. O VirtualBox tenta executar uma porção do código dos sistemas virtuais diretamente no processador. Para que sejam executadas as instruções privilegiadas, ele tenta mover o sistema operacional para o nível de ring 1, ao invés do ring 0. Como já visto, o nível de ring 1 geralmente não é utilizado na arquitetura x86. Caso haja problemas no processo, o VirtualBox também utiliza a técnica de recompilação dinâmica. O recompilador do VirtualBox é baseado no open-source QEMU. Adicionalmente, o VirtualBox automaticamente “desmonta” e, na maioria dos casos, “corrige” o código dos sistemas convidados a fim de prevenir futuras recompilações. Em razão disso o código executa nativamente na maior parte do tempo, numa tentativa de aumentar seu desempenho. No software, os discos são emulados em um recipiente especial chamado Virtual Disk Image (arquivos VDI), o qual até o momento é incompatível com formatos usados por outras soluções. O VirtualBox possui uma funcionalidade que pode conectar dispositivos iSCSI e usá-los como discos virtuais. O VirtualBox virtualiza os adaptadores gráficos como no padrão VESA e cuja memória pode ser ajustada. Em sistemas convidados Linux e Windows, é possível instalar drivers gráficos especiais para melhorar o desempenho. Os adaptadores de rede são virtualizados como adaptadores AMD PCNet, e placas de som como dispositivos Intel ICH AC97. Dispositivos USB também são emulados.

Outras características do VirtualBox são:

- \* Permite virtualização recursiva (uma instância do VirtualBox pode ser executada em sistema convidado).
- \* Permite controle total através de linha de comando.
- \* Permite logon automático em máquinas virtuais Windows.
- \* Inclui um servidor Microsoft Remote Desktop Protocol (RDP) para

administração de máquinas virtuais.

\* Inclui suporte total a Intel VT e suporte experimental ao AMD-V.

### 3.3. XEN

O Xen é uma plataforma de virtualização do tipo I para a arquitetura x86. Desenvolvido pela Citrix Systems Inc. O projeto Xen é de código aberto e baseado na General Public License (GPL). Foi originalmente parte fundamental de um projeto de pesquisa na Universidade de Cambridge chamado XenServer, cujo objetivo era “prover uma infra-estrutura pública para computação distribuída” [CLARK]. Ian Pratt, que foi líder do projeto, fundou a empresa XenSource Inc. que atualmente suporta o desenvolvimento do projeto open source e também possui versões comerciais do software.

O Xen utiliza o modelo de paravirtualização para prover máquinas virtuais. Como se sabe, a paravirtualização é o processo que simplifica a interface exportada para hardware de uma forma que elimina certas características que são difíceis de virtualizar. Um bom exemplo dessas características são as instruções sensíveis que possuem um comportamento diferente dependendo da forma que está executando nos modos usuário ou kernel. Um significativo overhead é gerado uma vez que as instruções devem ser interceptadas e interpretadas pela camada de virtualização. O Xen utiliza a paravirtualização para reduzir esse overhead [YOUSEFF et al]. A paravirtualização permite que máquinas virtuais específicas comuniquem-se diretamente com o hardware. Ao invés de todas as máquinas virtuais se comunicarem com o sistema anfitrião, é a máquina privilegiada que gerencia a interação e recebe as chamadas passadas pelos outros sistemas virtuais. Ele possui acesso privilegiado ao hardware e os sistemas convidados utilizam esse acesso privilegiado como uma espécie de ponte para acessar o hardware. A memória é separada em blocos pelo monitor de máquinas virtuais, e os sistemas convidados podem utilizar esses blocos da forma que lhes convier, tornando o acesso à memória direto e mais eficiente. Esta separação e isolamento também ocorrem em dispositivos como disco, o que proporciona um acesso mais rápido a estes. O monitor de máquinas virtuais só interfere quando ocorre um acesso fora do bloco [LAUREANO 2006].

É necessário que os sistemas operacionais sejam modificados para suportar esta virtualização, contudo não é necessário que as aplicações que executem sobre esses sistemas



sejam reescritas. Algumas distribuições Linux como o Red Hat e o Debian, já possuem suporte nativo ao Xen.

É importante lembrar que o Xen suporta (através de pacotes adicionais) que sistemas operacionais executem sem modificações, desde que o hardware possua processadores com a tecnologia de hardware, que será explicado mais adiante.

### **3.4. VIRTUAL PC**

O Virtual PC é um sistema virtualizador de PCs (*Personal Computer*), produzido pela Microsoft. O Virtual PC possui uma versão gratuita destinada a desktops e usuários comuns, popularmente conhecido como Microsoft Virtual PC 2007. Este software passou a ser gratuito em julho de 2006, quando o Virtual PC 2004 SP1 se tornou freeware. Já na versão 2007, o programa ficou mais desenvolvido, rápido e estável, passando a executar o Windows Vista de forma mais eficaz e dinâmica.

Seus concorrentes diretos são o VMware e VirtualBox, além dos menos utilizados, QEMU e Bochs, entre outros. Para executar o Windows na máquina virtual, sob um sistema Windows também, pode ser uma boa opção usar o Virtual PC. Seu uso é mais dirigido para usuários windows que necessitam executar uma outra versão deste sistema operacional.

Segundo o website GDH.NET.BR, “*Apesar da Microsoft ter lançado alguns drivers para Linux, (Virtual Machine Additions for Linux, para o MS Virtual Server 2005), seu desempenho não é tão satisfatório como muitos dizem, pelo menos*”. [GDH.NET.BR – 2010]

Para o Virtual PC 2007 não há opção de nenhum sistema operacional Linux no momento de criar uma máquina virtual.

O Virtual PC 2007 pode ser baixado gratuitamente em:

<http://www.microsoft.com/windows/products/winfamily/virtualpc/default.msp>.

#### 4. CONCLUSÃO

Ao observar a grande demanda de informações que trafegam por intermináveis redes de computadores, sistemas interligados e níveis de segurança cada vez mais exigidos, aliados a necessidade de redução de custos, espaço físico, entre outros fatores, entende-se que a virtualização, principalmente de servidores é uma das grandes evoluções da área de tecnologia da informação.

A virtualização de servidores possibilita a consolidação de servidores físicos, diminuindo o custo de operação de um Data Center, como upgrade de servidores, gerenciamento, consumo de energia, espaço físico e espaço para armazenamento de dados.

Permite também reduzir o número de equipamentos como PDUs, equipamentos de refrigeração de ar, etc.

Ao virtualizar os servidores, é possível reduzir o número de switches de redes, uma vez que são grandes consumidores de energia.

A virtualização de servidores proporciona alta disponibilidade para todos os servidores do ambiente, sem a necessidade de duplicação de hardware ou aquisição de licenças de software de clusterização, que possuem elevados valores.

Mesmo tendo que adquirir equipamentos de custos elevados como storages, a virtualização de servidores diminui drasticamente inúmeros problemas que um ambiente não virtualizado enfrenta, como recuperação de desastres, backups dos servidores, reinício de serviços parados, *downtime*, migração de servidores, além de poder realizar testes nos servidores.

Em caso de servidores que apresentam serviços parados, devido alguma falha, a virtualização possui ferramentas que são capazes de acionar outros servidores redundantes, para dar continuidade aos serviços, em muitas vezes, sem que o usuário ou sistemas detectem essa migração.

Mediante todas estas observações, conclui-se que a virtualização de servidores é muito eficaz e altamente importante para a continuidade de serviços por um maior tempo possível. Ao analisar os diversos benefícios e ferramentas que possibilitam a virtualização de servidores, afirma-se que a virtualização, através de todos os recursos disponíveis, é uma técnica que aumenta consideravelmente a eficácia e continuidade do ambiente computacional em pleno funcionamento.

Conclui-se também que, das diversas ferramentas de virtualização analisadas, a VMware foi a ferramenta que mais apresentou recursos de virtualização, sendo considerada a mais eficaz para essa finalidade.

## 5. REFERÊNCIAS BIBLIOGRÁFICAS

BRUNO KINOSHITA. Tecnologia da Informação – IT Expert disponível em [http://www.ecorpore.com/bruno/VMware\\_consolidated\\_backup.asp](http://www.ecorpore.com/bruno/VMware_consolidated_backup.asp) - Acesso em 11/10/2010 às 9h

COELHO, Fábio de Azevedo; CALZAVARA, Gustavo Santos; LUCIA, Ricardo di. Engenharia de Controle e Automação. Universidade Federal do Rio de Janeiro – Virtualização – VMware e Xen. Disponível em [http://www.gta.ufrj.br/grad/09\\_1/versao-final/virtualizacao/xen.html](http://www.gta.ufrj.br/grad/09_1/versao-final/virtualizacao/xen.html)  
Acesso em 08/09/2010 às 11h

GDH.NET.BR – Guia do Hardware.net – disponível em <http://www.guiadohardware.net/tutoriais/microsoft-virtual-pc/> - Acesso em 10/11/2010 às 15h

JUNIOR, Vitor Micillo - VIVA O LINUX – PORQUE NÓS AMAMOS A LIBERDADE disponível em <http://www.vivaolinux.com.br/artigo/Gerenciamento-remoto-de-servidores-VMWare-via-SSH> Acesso em 10/11/2010 às 11h30

MANFRIN, Alexandre. VM World Brazil – História: Conhecendo a origem da virtualização. Disponível disponível em [http://www.vmworld.com.br/br/index.php?option=com\\_content&view=article&id=80:historia-conhecendo-a-origem-da-virtualizacao&catid=50:virtualizacao](http://www.vmworld.com.br/br/index.php?option=com_content&view=article&id=80:historia-conhecendo-a-origem-da-virtualizacao&catid=50:virtualizacao). Acesso em 13/09/2010 às 12h

SEARCH SERVER VIRTUALIZATION.COM. Tecnologia da Informação – IT Expert disponível em [http://searchservervirtualization.techtarget.com/tip/0,289483,sid94\\_gci1379075,00.html](http://searchservervirtualization.techtarget.com/tip/0,289483,sid94_gci1379075,00.html) - Acesso em 11/10/2010 às 21h30

VMWARE. Conceitos básicos em virtualização. Disponível em <http://www.VMware.com/br/technology/history.html> e <http://www.vmware.com/br/products/>  
Acessos em 03/09/2010 às 16h e 09/09/2010 às 12h20

VMWARE. Infrastructure Resource Management Guide disponível em [http://www.vmware.com/support/pubs/vi\\_pubs.html](http://www.vmware.com/support/pubs/vi_pubs.html). Acesso em 01/10/2010 às 15h

VMWARE. VMware Infrastructure Installation and Upgrade Guide e Resource Management Guide disponível em [http://www.vmware.com/support/pubs/vi\\_pubs.html](http://www.vmware.com/support/pubs/vi_pubs.html). Acesso em 01/10/2010 às 16h45

VMWARE. VMware Infrastructure Basic System Administration Guide disponível em [http://www.vmware.com/support/pubs/vi\\_pubs.html](http://www.vmware.com/support/pubs/vi_pubs.html). Acesso em 02/10/2010 às 12h30

WATERS, John K. ABC da Virtualização - CIO – Estratégias de negócios e TI para líderes corporativos. Disponível em <http://cio.uol.com.br/tecnologia/2007/08/14/idgnoticia.2007-08-14.5515750576/> - Acesso em 11/08/2010 às 9h