

UNIVERSIDADE DO VALE DO RIO DOS SINOS - UNISINOS  
CIÊNCIAS EXATAS E TECNOLÓGICAS  
CURSO DE SEGURANÇA DA TECNOLOGIA DA INFORMAÇÃO

EDUARDO RECK FARIAS

MELHORES PRÁTICAS DE SEGURANÇA NO AMBIENTE DE VIRTUALIZAÇÃO

São Leopoldo

2007

EDUARDO RECK FARIAS

MELHORES PRÁTICAS DE SEGURANÇA NO AMBIENTE DE VIRTUALIZAÇÃO

Trabalho de conclusão de curso apresentado à  
Universidade do Vale do Rio dos Sinos –  
UNISINOS, como requisito parcial para a  
obtenção do título de Tecnólogo em Segurança  
da Informação.

Orientador: Prof. Ms. Glauco Antonio Ludwig

São Leopoldo

2007

*Dedico esse trabalho aos meus Pais.  
Sem eles, nada disso seria possível.*

## **AGRADECIMENTOS**

Agradeço a Deus pela vida. Porém, sem meus Pais, Elaine e Francisco, eu não teria as oportunidades que tive para poder estar me formando. Agradeço também ao meu irmão Henrique pelo companheirismo e camaradagem. Por último, e não menos importante, agradeço minha namorada Mariana pela compreensão dispensada nessa etapa. Amo vocês quatro pra sempre.

Agradeço também pela amizade, e principalmente pela paciência, do meu orientador Prof. Ms. Glauco Antonio Ludwig.

"Há homens que lutam um dia e são bons.  
Há outros que lutam um ano e são melhores.  
Há os que lutam muitos anos e são muito bons.  
Porém, há os que lutam toda a vida.  
Esses são os imprescindíveis."

Bertolt Brecht

## RESUMO

Nas últimas décadas tem-se notado o avanço tanto das pesquisas como da utilização da virtualização nos ambientes computacionais. Esse crescimento da virtualização foi e é fomentado tanto pelas áreas acadêmicas, como pelas empresas que apostaram nessa tecnologia. Além de utilizar a virtualização para resolver problemas como, por exemplo, a subutilização dos hardwares, as organizações têm experimentado a virtualização como sendo uma nova alternativa para ajudar a manter os ambientes computacionais mais estáveis e seguros. Esse trabalho aborda as boas práticas de segurança que devem ser aplicadas em um ambiente virtualizado, bem como as ferramentas que estão disponíveis para que a virtualização torne-se um componente de segurança fundamental na proteção contra ataques e falhas. Com isso espera-se mitigar as ameaças que venham a comprometer os pilares da segurança.

**Palavras-Chave:** Máquinas Virtuais. Segurança. Melhores Práticas.

## ABSTRACT

*During the last decades the advance of researches as of the virtualization usage have been noticed into computational environment. This virtualization growth was and it is fomented much as for the academic areas as for the corporations, that bet on this technology. Beyond the virtualization usage to solve problems, as for example, hardware underused, organizations have been experienced virtualization as a new alternative to keep their computational environments more stable and secure. This term broachs security best practices which must be applied into a virtualization environment, as well as tools which are available to turn virtualization as a fundamental security component on protection against attacks and failures. By this way it is supposed to mitigate threats that could compromise the security pillars.*

**Keywords:** *Virtual Machines. Security. Best Practices.*

## LISTA DE FIGURAS

<b>Figura 1:</b> Arquitetura Tipo I.....	17
<b>Figura 2:</b> Arquitetura Tipo II.....	17
<b>Figura 3:</b> Desempenho de classes de máquinas virtuais.....	20
<b>Figura 4:</b> Processo de instalação e configuração de 4 servidores sem o uso de clone ..	22
<b>Figura 5:</b> Processo de instalação e configuração de 4 servidores com o uso do clone..	22
<b>Figura 6:</b> Exemplo de arquitetura virtual de rede.....	28
<b>Figura 7:</b> Exemplo de integração dos componentes do ambiente virtual .....	29
<b>Figura 8:</b> Diferença na arquitetura da <i>Service Console</i> nas versões ESX 2 e ESX 3....	30
<b>Figura 9:</b> Exemplo do funcionamento da ferramenta VMotion .....	43
<b>Figura 10:</b> Exemplo do funcionamento da ferramenta HA.....	44
<b>Figura 11:</b> Exemplo do funcionamento da ferramenta DRS.....	45
<b>Figura 12:</b> Exemplo do funcionamento da ferramenta <i>Consolidated Backup</i> .....	46
<b>Figura 13:</b> Integração das funcionalidades DRS, HA e CB ao ambiente virtual. ....	46
<b>Figura 14:</b> Ambiente computacional atual da Fundação CEEE.....	56
<b>Figura 15:</b> Ambiente computacional projetado para a Fundação CEEE .....	63



## LISTA DE ABREVIATURAS E SIGLAS

**AES** - *Advanced Encryption Standard*

**API** - *Application Programming Interface*

**ARP** - *Address Resolution Protocol*

**CCEVS** - *Common Criteria Evaluation and Validation Scheme*

**COS** - *Console OS*

**CP/CMS** - *Control Program / Conversational Monitor System*

**CSIM** - *Complete Software Interpreter Machine*

**CTSS** - *Compatible Time-Sharing System*

**DMZ** - *DeMilitarized Zone*

**DRS** - *Distributed Resource Scheduler*

**EAL** - *Evaluation Assurance Level*

**FTP** - *File Transfer Protocol*

**HA** - *High Availability*

**HBA** - *Host Bus Adapter*

**HP** - *Hewllet-Packard*

**HTTP** - *HyperText Tranfer Protocol*

**HTTPS** - *HyperText Tranfer Protocol Secure*

**HVM** - *Hybrid Virtual Machine*

**IP** - *Internet Protocol*

**iSCSI** - *Internet Small Computer System Interface*

**LAN** - *Local Area Network*

**MAC** - *Media Access Control*

**M.I.T** - *Massachusetts Institute of Technology*

**NIC** - *Network Interface Card*

**NIS** - *Network Information Service*

**NSA** - *National Security Agency*

**PATA** - *Parallel Advanced Technology Attachment*

**RAID** - *Redundant Array of Independent Drives*

**RAM** - *Random Access Memory*

**RPM** - *Red Hat Package Manager*

**RSA** - *Ron Rivest, Adi Shamir e Leonard Adleman*

**SAN** - *Storage Area Network*

**SAS** - *Serial Attached SCSI*

**SCSI** - *Small Computer System Interface*

**SNMP** - *Simple Network Management Protocol*

**SSH** - *Secure Shell*

**SSL** - *Secure Socket Layer*

**TCP** - *Transmission Control Protocol*

**VI** - *Virtual Infrastructure*

**VLAN** - *Virtual LAN*

**VMFS** - *Virtual Machine File System*

**VMM** - *Virtual Machine Monitor*

## SUMÁRIO

<b>1 INTRODUÇÃO.....</b>	<b>11</b>
<b>2 REFERENCIAL TEÓRICO .....</b>	<b>14</b>
2.1 DEFINIÇÃO DE MÁQUINA VIRTUAL .....	14
2.2 ORIGEM DAS MÁQUINAS VIRTUAIS .....	14
2.3 O <i>VIRTUAL MACHINE MONITOR</i> .....	16
2.4 CLASSES DE MÁQUINAS VIRTUAIS .....	19
2.5 VANTAGENS E DESVANTAGENS DAS MÁQUINAS VIRTUAIS.....	20
2.5.1 Vantagens no Uso de Máquinas Virtuais .....	20
2.5.2 Desvantagens no Uso de Máquinas Virtuais .....	24
<b>3 SEGURANÇA POR VIRTUALIZAÇÃO.....</b>	<b>26</b>
3.1 SEGURANÇA DOS COMPONENTES BÁSICOS DO AMBIENTE VIRTUAL.....	28
3.1.1 Proteção da <i>Service Console</i> .....	29
3.1.2 Proteção do host VMware ESX Server .....	35
3.1.3 Proteção das Máquinas Virtuais.....	37
3.1.4 Proteção do VMware VirtualCenter Server .....	39
3.2 FERRAMENTAS DISPONÍVEIS PARA O AMBIENTE VIRTUAL .....	41
3.2.1 Movimentação de Máquinas Virtuais <i>On-line</i> .....	42
3.2.2 Alta-disponibilidade das Máquinas Virtuais.....	44
3.2.3 Balanceamento de carga entre os servidores VMware ESX Server.....	45
3.2.4 <i>Backup</i> do Ambiente Virtual .....	45
<b>4 DISPONIBILIDADE, CONFIDENCIALIDADE E INTEGRIDADE.....</b>	<b>47</b>
4.1 DISPONIBILIDADE .....	47
4.2 CONFIDENCIALIDADE .....	50
4.3 INTEGRIDADE .....	52
<b>5 ESTUDO DE CASO.....</b>	<b>55</b>
5.1 INFORMAÇÕES DA EMPRESA.....	55
5.2 CENÁRIO ATUAL .....	56
5.3 NECESSIDADES ATUAIS DA EMPRESA.....	60
<b>6 CONCLUSÃO.....</b>	<b>64</b>
<b>REFERÊNCIAS.....</b>	<b>66</b>

## 1 INTRODUÇÃO

As máquinas virtuais (*virtual machines* - VM) foram idealizadas e introduzidas nas décadas de 50 e 60, com a finalidade de permitir o *time-sharing*<sup>1</sup> de equipamentos que eram muito caros e ficavam, por vezes, ociosos por muito tempo. A principal proposta do compartilhamento de hardware era prover a máxima utilização dos equipamentos Mainframe da IBM de forma segura, conseguindo assim aperfeiçoar o uso do hardware entre vários usuários [1]. Desde então, as tecnologias de virtualização vêm sendo aprimoradas cada vez mais, tendo em vista a grande aceitação por parte das empresas e dos usuários. Em pesquisa realizada pelo IDC Brasil, em Setembro de 2006 [2], 80% das grandes e médias empresas brasileiras investiram em virtualização. Já o Instituto de Pesquisas Gartner, diz que o número total de máquinas virtuais em execução, registradas até o final de 2006, pode saltar de 540 mil para mais 4 milhões até 2009 [3]. Tal avanço na utilização de máquinas virtuais foi promovido em função de vários benefícios como: a redução do custo de propriedade, as ferramentas de alta-disponibilidade que esta tecnologia oferece e por ser mais uma forma de prover segurança aos serviços críticos das organizações.

Pelo crescente uso e aceitação dos sistemas de informatização, as empresas têm virtualizado cada vez mais sistemas críticos aos seus negócios, tornando a virtualização uma peça de fundamental importância para a continuidade da operação desses negócios. Exemplos da aplicação de máquinas virtuais são bastante comuns, seja para prover alta-disponibilidade para servidores de missão crítica, seja em ambientes de treinamento e de desenvolvimento e, também, como novas opções de recuperação de desastres. Além disso, com a virtualização, tem-se um leque de ferramentas que ajudam a aumentar a segurança do ambiente virtual.

Hoje em dia, as empresas não estão somente procurando obter/utilizar todas as facilidades que a virtualização traz aos ambientes computacionais. Estas empresas, ou usuários, também estão preocupados se com a virtualização dos ambientes computacionais pode-se garantir um, ou mais, dos três princípios básicos da segurança: a) confidencialidade, b) disponibilidade e c) integridade (tanto das máquinas virtuais como do hardware que as suportam). Por exemplo, ao instanciar três máquinas virtuais críticas em um mesmo hardware físico, como: banco de dados de faturamento, serviço de correio eletrônico e o *firewall* corporativo, um erro de programação no banco de dados poderia ocasionar uma utilização

---

<sup>1</sup> Capacidade de múltiplos usuários compartilharem recursos computacionais de uma única origem.

excessiva de memória nessa máquina virtual. Esse uso excessivo de memória poderia propagar-se para as outras máquinas virtuais, fazendo com que todas apresentassem um comportamento fora do padrão e deixassem de prover os seus respectivos serviços a uma corporação. Assim, torna-se uma questão sensível a garantia de que ao se colocar vários serviços críticos virtualizados sobre um mesmo hardware físico, uma falha ou um ataque, em uma determinada máquina virtual, não venha a comprometer o funcionamento de outras máquinas virtuais, ou até mesmo o funcionamento do hardware onde as mesmas estão instanciadas.

Em meio ao cenário atual da informatização das empresas, em que a tecnologia da informação vem agregando mais valor aos negócios e dando cada vez mais suporte aos mesmos, empresas que optam pela virtualização de seu ambiente computacional não podem estar suscetíveis às ameaças de indisponibilidade dos seus serviços. Tais ameaças podem ser tanto uma falha do hardware físico, uma manutenção programada de servidores, ou até mesmo um ataque de negação de serviço. Atualmente prover confidencialidade, disponibilidade e integridade para serviços que são executados em hardware real e dedicados, tornam-se caro e exigem um nível de conhecimento alto, visto a complexidade das aplicações que dão suporte a este fim.

Ao utilizar a virtualização, benefícios como a redução do custo de propriedade, mobilidade, alta-disponibilidade e rápida recuperação de desastres ficam à disposição das empresas. Porém, o simples fato de optar-se pela virtualização não garante de forma integral que os princípios básicos de segurança serão alcançados. Para que todos, ou a maioria, destes princípios/objetivos sejam conquistados com êxito, faz-se necessário o uso de boas práticas de segurança e ferramentas disponíveis para o ambiente virtual.

Assim, o principal objetivo deste trabalho é elencar as boas práticas de segurança que devem ser utilizadas em um ambiente virtualizado. Além disso, também será alvo de estudo desse trabalho a forma que a virtualização pode ser empregada, bem como as ferramentas que estão disponíveis para a mesma, como sendo mais uma forma de aumentar a segurança do ambiente computacional. Após elencar as boas práticas e descrever como a virtualização pode ajudar a aumentar a segurança, esses conceitos identificados serão aplicados em um estudo de caso. Nesse estudo de caso será realizado um projeto de virtualização do ambiente computacional de uma organização, utilizando as boas práticas de segurança e as ferramentas disponíveis para o ambiente virtual. Assim, espera-se mitigar as ameaças que venham a comprometer os pilares de segurança da organização que será alvo do estudo de caso.

A estrutura do trabalho será organizada da seguinte forma: No Capítulo 2 é apresentada a definição de máquina virtual, bem como sua origem, classes, vantagens e desvantagens. No Capítulo 3 são elencados os fatores que fazem com que o ambiente virtual torne-se tão ou mais seguro que o ambiente tradicional de computação. No próximo capítulo são co-relacionadas as boas práticas de segurança no ambiente virtual para que consiga-se garantir disponibilidade, confidencialidade e integridade para o ambiente virtual. O estudo de caso será descrito no Capítulo 5, no qual se apresentam informações sobre a empresa analisada, ambiente atual, necessidades de melhorias na segurança e o ambiente virtual proposto para suprir essas necessidades. O Capítulo 6 é onde serão feitas as conclusões desse trabalho e perspectivas de trabalhos futuros. E, por fim, as referências bibliográficas são apresentadas.

## 2 REFERENCIAL TEÓRICO

Nesse capítulo são abordadas algumas definições do que é uma máquina virtual. Para tal, faz-se necessário descrever a origem das mesmas, desde os primeiros ensaios da década de 50 até os dias atuais. Além disso, será feita uma abordagem da definição do que é a camada de virtualização, comumente chamada de *Virtual Machine Monitor* (VMM). Será feita uma breve descrição das classes de máquinas virtuais. E, finalizando o capítulo, serão listadas as vantagens e desvantagens da utilização de máquinas virtuais.

### 2.1 DEFINIÇÃO DE MÁQUINA VIRTUAL

Uma máquina virtual, segundo Wright [4], pode ser conceituada como uma abstração de software que enxerga e acredita residir sobre um sistema físico. Ou seja, máquinas virtuais são cópias virtualizadas e isoladas deste sistema físico, com a finalidade de compartilhar os recursos de hardware do mesmo. Com isso, é possível a convivência de sistemas operacionais totalmente diferentes em um mesmo equipamento, isto porque cada máquina virtual possui os seus próprios dispositivos virtualizados. Isso quer dizer que para cada máquina virtual é criado um ambiente isolado.

### 2.2 ORIGEM DAS MÁQUINAS VIRTUAIS

Os princípios de virtualização foram idealizados no final da década de 50 pelo *Massachusetts Institute of Technology* (M.I.T.). Neste período o M.I.T deu início ao estudo do *time-sharing*, chamando na época de *Compatible Time-Sharing System* (CTSS). Já no início da década de 60, pesquisadores da IBM começaram a avaliar os emergentes conceitos do CTSS. Nessa época a IBM buscava um ambiente isolado onde se pudesse realizar algumas avaliações e testes. Para este fim, a IBM Yorktown Research Center começou a desenvolver um método para dividir o hardware, ou seja, particionar o equipamento em partes menores e isoladas. Estas partes, por sua vez, tinham a capacidade de gerenciamento dos recursos

divididos que eram entregues a estas micro-partições do equipamento. Com posse destes particionamentos isolados, os pesquisadores puderam realizar, de forma concorrente, os seus testes nas mais diversas condições. Todos esses testes foram executados sem que os processos de cada micro-particionamento pudessem afetar as outras partes que se encontravam no sistema. Assim, a versão final do CTSS, nomeado de TSS/360, chegou a ser lançada. Contudo, o mesmo era um sistema que exigia muitos recursos do hardware onde era instalado.

Com base no aprendizado obtido pelos experimentos realizados, a IBM desenvolveu, no início da década de 70, um sistema operacional completamente diferente. Este, por sua vez, tinha o objetivo de prover as duas principais funções do CTSS, a multiprogramação e a máquina estendida. Na época foi chamado de *Control Program / Conversational Monitor System* (CP/CMS respectivamente), e, posteriormente veio a chamar-se VM/370. O CP era um sistema operacional capaz de simular múltiplas cópias idênticas dele mesmo, incluindo, por exemplo, as interrupções, em um único hardware. Já o CMS, era um sistema operacional que suportava o uso interativo por um usuário (o CMS na verdade era o típico sistema operacional convidado que reside dentro da máquina virtual). O cerne deste novo sistema desenvolvido era o *Virtual Machine Monitor* (VMM). Assim, com o VM/370 tornava-se possível a criação de máquinas virtuais.

Com as inovações propostas no conceito das máquinas virtuais é que a IBM deu o passo inicial para a comercialização do sistema operacional para ambientes multi-usuários. Os equipamentos IBM *System 370* e *390* começavam a fazer uso do sistema operacional IBM VM/ESA, o qual já era capaz de instanciar máquinas virtuais. Porém, a virtualização ainda não tinha seu espaço nos ambientes computacionais. Devido ao alto custo dos hardwares, para aquela época, que podiam suportar o particionamento lógico de seus recursos. Após o período de lançamento dos IBM *System 370* e *390*, até a década de 80, a virtualização praticamente não teve desenvolvimento, tão pouco fora usada em ambientes de produção. Atualmente, o desenvolvimento de sistemas de virtualização está voltado quase que em sua totalidade para a arquitetura x86, e não mais para arquiteturas *Mainframes*.

Após 1980 foi que a virtualização começou a renascer. Este renascimento deve-se, em grande parte, a duas frentes de utilização: a) a industrial com VMware [10]; e b) a acadêmica XEN [27] e Plex86 [28].

Além dessas duas frentes de utilização, outros fatores fizeram com que a virtualização se tornasse uma das tecnologias mais promissoras das últimas duas décadas. Um destes fatores foi a progressiva queda do custo do hardware. Com esta queda do custo, houve uma



proliferação de hardware dentro das empresas, isto porque os administradores temiam em colocar mais de um serviço para serem executados sobre um mesmo hardware físico. Este receio era em função de que um serviço viesse a comprometer o funcionamento dos demais serviços executados no mesmo equipamento.

Tendo em vista um cenário quase que caótico, mais problemas surgiram com o aumento descontrolado do ambiente computacional, como a subutilização dos servidores físicos, a complexidade no gerenciamento dos servidores e a falta de espaço físico para colocação destes servidores. Em pesquisa realizada pela Service IT Solutions [20] em 2005, a carga que um serviço gera quando executado em um hardware dedicado somente a ele chega a até 15%, ou seja, as empresas começaram a perceber uma perda de 85% no investimento em hardware. Em meio a isso, a virtualização veio para resolver também este problema. Ou seja, promover uma máxima utilização do hardware, fazendo assim com que as empresas tivessem que investir menos em recursos de hardware (reduzindo assim o custo total de propriedade).

Avançando na utilização da virtualização, a mesma mostra-se mais do que um facilitador para o aperfeiçoamento de recursos de hardware como fora proposto inicialmente, e sim, também, como uma nova solução para prover segurança para todo o ambiente computacional.

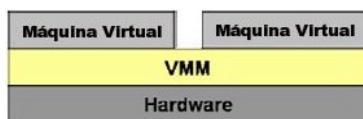
## 2.3 O VIRTUAL MACHINE MONITOR

O *Virtual Machine Monitor* (VMM) é uma camada de software que suporta a execução concorrente de múltiplas máquinas virtuais [5]. Já Kelem e Feiertag [6], em 1991, denominou o VMM como sendo um "sistema operacional para sistemas operacionais" ou, ainda, como sendo o VMM o responsável pela abstração de hardware que é entregue às máquinas virtuais. O VMM é o responsável por criar "uma ilusão" e prover as funcionalidades necessárias para que o sistema operacional convidado<sup>2</sup> (*guest operating system*) acredite estar sendo executado em um hardware real e dedicado somente para ele. Existem dois tipos de arquiteturas básicas para a construção de máquinas virtuais, são elas: tipo I e tipo II. Como pode ser visto na Figura 1, sistemas do tipo I são aqueles em que a camada de abstração de hardware (VMM) roda diretamente sobre o mesmo, ou seja, entre as

---

<sup>2</sup> Sistema operacional que é instalado e reside dentro de uma máquina virtual.

máquinas virtuais e os recursos de hardware disponíveis. Já os sistemas do tipo II, como estão exemplificados na Figura 2, são aqueles em que o *monitor* (VMM) é executado como um processo entre a máquina virtual e o sistema operacional hospedeiro<sup>3</sup> (*host operating system*), ou seja, existe uma camada adicional para fazer o acesso ao hardware.



**Figura 1:** Arquitetura Tipo I

**Fonte:** Adaptado de MAIA, 2005, p 13.



**Figura 2:** Arquitetura Tipo II

**Fonte:** Adaptado de MAIA, 2005, p 13.

Segundo Robin e Irvine [7], o VMM faz o gerenciamento dos recursos reais do hardware físico, exportando-os para as máquinas virtuais. Para que o VMM pudesse prover estas vantagens, o mesmo foi concebido sobre três pilares, compatibilidade, desempenho e simplicidade.

A compatibilidade é fundamental, pois além do suporte a sistemas legados que serão executados dentro das máquinas virtuais, é uma característica necessária para que seja possível a movimentação de máquinas virtuais entre hardwares de diferentes fabricantes, fazendo assim com que a máquina virtual seja executada sem erro algum após a troca de hardware físico.

O desempenho foi alcançado basicamente fazendo com que a máquina virtual fosse executada na mesma velocidade com que um *software* qualquer fosse executado sobre um hardware dedicado. Por fim, a simplicidade é particularmente importante, pois caso o VMM tivesse seu cerne complexo, um erro no *kernel* do mesmo, poderia causar a parada de todas as máquinas virtuais em execução.

Com relação à segurança em prover o real isolamento entre as máquinas virtuais, o VMM precisa ser livre de erros de programação, onde tais erros poderiam ser utilizados por um atacante para comprometer o sistema.

<sup>3</sup> Sistema operacional sobre o qual o VMM é executado.

Whitaker [5] expandiu os benefícios na utilização do VMM. São eles:

- Simplicidade e estabilidade da API: comparado com sistemas operacionais monolíticos, o VMM oferece uma interface de sistema que é significativamente menor e mais estável. Isso ocorre, porque o VMM não faz nenhuma exigência funcional que não seja virtualizar o hardware físico;
- Suporte a sistemas operacionais e aplicativos antigos: o VMM suporta a execução de sistemas operacionais e aplicações antigas;
- Capacidade de executar sistemas completos: através da virtualização da camada de hardware, o VMM suporta a execução de sistemas completos. Ou seja, o conjunto formado pelo sistema operacional mais a coleção de aplicações, as bibliotecas compartilhadas e os demais componentes. Esta capacidade permite a migração de sistemas completos, incluindo todas as aplicações e o estado atual do sistema;
- Implementação baseada em software: a implementação baseada em software, por si só, proporciona vários benefícios. Entre eles é possível destacar a agilidade proporcionada com a utilização de máquinas virtuais, ou seja, elas podem rapidamente ser ligadas, desligadas e instanciadas sem os incômodos das máquinas físicas. Além disso, em função do VMM propiciar a arquitetura de hardware em software, existe uma maior facilidade para desenvolver e testar mudanças para a abstração de hardware.

Para Robin e Irvine [7], o VMM possui outras três características básicas que devem ser destacadas:

- Ambiente de execução quase idêntico à máquina original: qualquer programa que execute sobre uma máquina virtual deve ser capaz de executar sobre a máquina real;
- Possuir controle dos recursos reais do sistema: nenhum programa que rode sobre um VMM pode acessar qualquer recurso que não tenha sido explicitamente alocado para este VMM. Além disso, um VMM pode recuperar o controle de recursos previamente alocados;
- Eficiência: um grande percentual das instruções do processador virtual deve ser executado pelo processador da máquina real, sem a intervenção do VMM. Porém,

as instruções que não podem ser executadas diretamente pelo processador real são interpretadas pelo VMM.

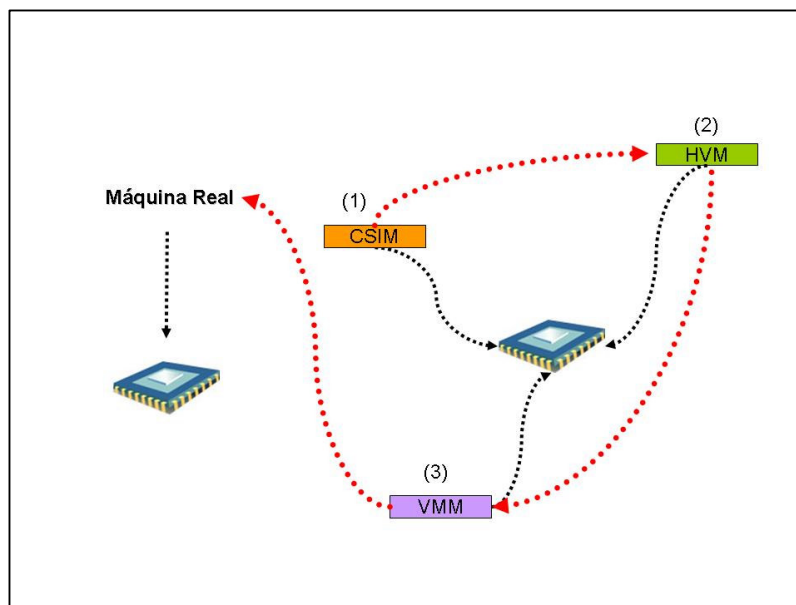
## 2.4 CLASSES DE MÁQUINAS VIRTUAIS

McEwan [8] dividiu as tecnologias de máquinas virtuais em: a) *Complete Software Interpreter Machine* (CSIM); b) *Virtual Machine Monitor* (VMM) e; c) *Hybrid Virtual Machine* (HVM). Para determinar a classe de uma determinada máquina virtual, faz-se necessário avaliar o conjunto de software que é executado através de instruções do processador. Em uma máquina real, por exemplo, o processador executa as instruções dos aplicativos diretamente.

Uma máquina virtual pode pertencer a um dos grupos citados abaixo:

- *Complete Software Interpreter Machine* (CSIM): usa somente interpretação por software. Ou seja, um programa emula cada instrução do processador. Possui como principal exemplo a máquina virtual Bochs [9];
- VMM: necessita que um subconjunto de instruções privilegiadas do processador virtual seja executado pelo processador real. Um exemplo de máquina virtual VMM são as máquinas criadas no VMware [10];
- *Hybrid Virtual Machine* (HVM): é uma VMM que usa interpretação por software sobre todas as instruções privilegiadas.

A Figura 3 ilustra como é, na avaliação de Robin e Irvine [7], o desempenho das três classes de máquinas virtuais. Onde a classe de máquinas virtuais que tem menor desempenho é a CSIM (1), pois precisa emular cada instrução ao processador. A classe que tem um desempenho melhor que o CSIM é a HVM (2), onde esta utiliza a interpretação por software para todas as instruções privilegiadas. Já o VMM (3) é a classe que possui o melhor desempenho, pois necessita que somente um subconjunto de instruções privilegiadas seja executado pelo processador real.



**Figura 3:** Desempenho de classes de máquinas virtuais

**Fonte:** Adaptado de MAIA, 2005, p. 15.

## 2.5 VANTAGENS E DESVANTAGENS DAS MÁQUINAS VIRTUAIS

Como descrito no Capítulo 1, ao se fazer a opção pelo uso da virtualização, novos horizontes são abertos pelas funcionalidades e facilidades trazidas pelo particionamento de servidores físicos. Esta etapa do trabalho irá abordar questões como vantagens, desvantagens e aplicabilidade do uso desta tecnologia.

### 2.5.1 Vantagens no Uso de Máquinas Virtuais

Um exemplo claro de como a virtualização pode ajudar a aumentar a disponibilidade com um baixo investimento em hardware é, por exemplo, considerando-se o seguinte cenário: em um *datacenter* existem quatro servidores físicos e cada um desses servidores executa um único serviço. Esses quatro serviços são vitais para os negócios da empresa. Ao se propor uma solução de cluster tradicional, seria necessária a aquisição de pelo menos mais quatro servidores, independente do tipo de cluster que será utilizado, ativo/ativo ou ativo/passivo. Nesse ambiente seriam necessários  $2 * N$  número de servidores para a composição do cluster,

ou seja, o dobro do número de servidores. Com isso seria preciso o dobro de investimento em hardware. Contudo, ao se trazer a virtualização para este cenário, pode-se prover o mesmo tipo de cluster, ativo/ativo ou ativo/passivo, com um número de servidores físicos igual a  $N + 1$ . Ou seja, se antes seriam necessários oito servidores físicos em uma arquitetura tradicional, com a virtualização são necessários apenas cinco servidores.

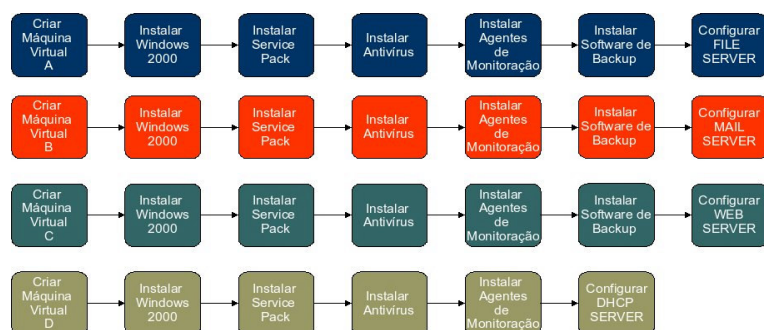
Outro exemplo, bastante comum, é quando uma instituição que já possui servidores virtuais em execução faz a aquisição de uma área de armazenamento externo. Para fazer com que as máquinas virtuais façam o uso desta área de armazenamento externo, faz-se necessária a aquisição de uma única interface *fiber channel*. Isso porque a mesma será compartilhada entre todas as máquinas virtuais instanciadas sobre o mesmo hardware físico (servidor). Em uma necessidade de balanceamento de carga e alta-disponibilidade de acesso à área de armazenamento externo, seria preciso a aquisição de somente mais uma interface *fiber channel*, totalizando duas interfaces apenas. Em um modelo tradicional de servidores, ou seja, sem a presença da virtualização, seria necessário um número de interfaces igual à quantidade de servidores físicos. Isto é, no ambiente tradicional, se dez servidores físicos precisarem de acesso a essa área externa, serão necessárias dez interfaces, uma para cada servidor. Ou seja, um número ainda cinco vezes maior de interfaces do que seria utilizado com a virtualização.

Uma das maiores vantagens de se ter um ambiente virtualizado é a mobilidade que o mesmo proporciona. Isso porque, seja qual for o hardware físico onde a máquina virtual é instanciada, a mesma visualizará sempre o mesmo hardware virtual. Ou seja, se uma máquina virtual é criada em um servidor IBM, essa pode ser movimentada para um servidor HP, mesmo que este novo servidor possua todos os recursos físicos (interfaces de rede e controladoras de disco, por exemplo) de outros fabricantes e/ou modelos. Com essa independência de hardware, a virtualização vem sendo empregada cada vez mais em *sites* de contingência de sistemas legados. Esses sistemas legados normalmente são executados em hardwares mais antigos, e, a aquisição desses mesmos equipamentos (hardware antigos), pode inviabilizar a utilização de um *site* de backup por serem mais caros. Ao virtualizar o sistema legado, o mesmo pode ser executado em um hardware mais novo. Além de prover o contingenciamento adequado, ao ser virtualizado em um hardware mais atual, o sistema está ganhando também em desempenho.

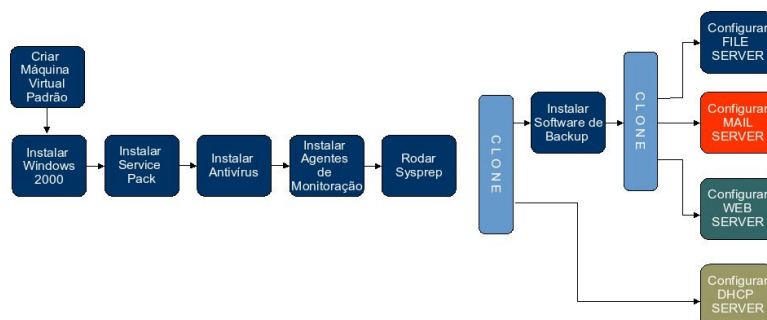
A provisão de novos servidores pode ser citada também como uma grande vantagem. Quando as instituições necessitam de um novo servidor, seja para homologação de alguma aplicação ou mesmo para que seja colocado em produção, está falando-se em dias ou até

mesmo semanas para a aquisição do servidor. Com a virtualização é possível o uso da clonagem, ou seja, é possível construir uma máquina virtual que servirá de modelo para as demais. Assim, quando for preciso provisionar um novo servidor, faz-se somente uma cópia desse modelo. Com isso, não será mais necessário realizar o orçamento de um novo equipamento, enviar para o setor de compras para que seja aprovado, esperar dias para que o servidor chegue para então começar a instalação e configuração do mesmo.

A seguir está exemplificado como a virtualização pode reduzir o tempo necessário para a instalação e configuração de um novo servidor. A Figura 4 mostra o processo desde a instalação do sistema operacional até a configuração final do serviço que será executado pelo servidor. Nessa figura são mostradas essas etapas em quatro servidores virtuais sem o uso da clonagem, ou como seria realizado se fosse a um ambiente tradicional. A soma das etapas resulta em 27 passos que devem ser realizados. Já a Figura 5 mostra a instalação e configuração dos mesmos quatro servidores, mas com o uso da clonagem, onde se tem ao todo 13 passos somente.



**Figura 4:** Processo de instalação e configuração de 4 servidores sem o uso de clone  
**Fonte:** SERVICE IT SOLUTIONS, 2007.



**Figura 5:** Processo de instalação e configuração de 4 servidores com o uso do clone  
**Fonte:** SERVICE IT SOLUTIONS, 2007.

Além das vantagens citadas anteriormente, existem ainda outras que de um modo geral, também justificam a utilização da virtualização. São elas:

- Pode ser utilizada para consolidar a carga de trabalho de vários servidores em poucos servidores, ou até mesmo, em um único servidor. Dessa forma, além de propiciar um melhor aproveitamento do hardware, promovem a redução dos custos de gerenciamento da infra-estrutura de hardware;
- Fornece isolamento de aplicações. Em muitos casos, ocorrem incompatibilidades entre as aplicações que rodam em um mesmo servidor físico. Com a utilização das máquinas virtuais é possível isolar as aplicações em máquinas virtuais distintas;
- Pode ser usada para prover segurança e isolamento para que aplicações não confiáveis sejam executadas;
- Simula configurações e situações diferentes do mundo real, como, por exemplo, se adicionada mais memória ou mais processadores na máquina virtual, pode-se prever o comportamento das aplicações que nela estão instaladas;
- Cria a ilusão de dispositivos de hardware que não existem no sistema, como, por exemplo, dispositivo *Small Computer System Interface* (SCSI) e múltiplos processadores;
- Permite que a conexão entre as máquinas virtuais e o sistema operacional hospedeiro, por se tratar de uma comunicação feita em memória, seja muito mais veloz do que a comunicação obtida através dos segmentos de redes convencionais;
- Pode ser usada para executar múltiplos sistemas operacionais simultaneamente. Desta forma, é possível testar a compatibilidade de hardware;
- Permite uma completa análise dos erros das máquinas virtuais, bem como a monitoração de desempenho dos sistemas operacionais. Isso, sem a perda de produtividade que ocorre nos sistemas reais;
- É ótima ferramenta para pesquisas e experiências acadêmicas. Isto porque as mesmas possuem o isolamento necessário para se efetuar estes experimentos;
- Garante a portabilidade das aplicações legadas (que executariam sobre uma máquina virtual simulando o sistema operacional original);
- Simula alterações e falhas de hardware para testes ou re-configuração de um sistema operacional, provendo confiabilidade e escalabilidade para as aplicações;
- Proporciona aperfeiçoamento e testes de novos sistemas operacionais;



- Ensino prático de sistemas operacionais e programação;
- Desenvolvimento de novas aplicações para diversas plataformas, garantindo a portabilidade destas aplicações.

### 2.5.2 Desvantagens no Uso de Máquinas Virtuais

Embora existam inúmeras vantagens que fomentam o uso das máquinas virtuais, não se pode deixar de mencionar as desvantagens.

No caso do uso da virtualização, existe a concentração do risco, ou seja, colocar vários serviços críticos para os negócios da empresa sobre máquinas virtuais em um ou alguns poucos servidores de virtualização (o que torna uma questão sensível à continuidade do negócio). Assim, caso uma falha física ocorra, todas as máquinas virtuais daquele sistema podem vir a ser comprometidas. Mesmo que atualmente a qualidade do hardware adquirido seja muito boa, o mesmo não está livre da ocorrência de falhas.

Para minimizar o impacto causado por essas falhas, é bastante comum o uso de módulos redundantes nos servidores físicos. Estes módulos podem ser duas fontes de energia, duas interfaces de rede, duas controladoras *fiber channel* e arranjo de discos (como espelhamento, por exemplo). Porém, ao se fazer a opção por um servidor que tenha a maior parte de seus recursos duplicados, faz-se com que o custo do mesmo aumente. Toda essa redundância tem um preço, e, cada componente de hardware que se provê duplicidade, encarece o valor total do equipamento. O preço do custo de recursos de hardware duplicados é uma das desvantagens da utilização de máquinas virtuais.

Outra desvantagem trazida pelo uso de máquinas virtuais diz respeito à questão de desempenho. Fica evidente que ao se usar uma camada adicional (o VMM) entre a máquina virtual e o hardware físico do servidor ocorre uma perda de rendimento. Por este motivo, existem aplicações que são mais, ou menos, indicadas a serem virtualizadas, dependendo do grau de utilização da mesma. Por isso, torna-se imprescindível um planejamento bem realizado para que não ocorra um gargalo em algum dos recursos de hardware, afetando assim o desempenho da máquina virtual em questão.

De um modo geral, as desvantagens na utilização das máquinas virtuais, seja ela a concentração de risco ou o desempenho, não são fatores que inviabilizam o seu uso. Isso ocorre em função dos diversos benefícios que são proporcionados com a sua utilização.

### 3 SEGURANÇA POR VIRTUALIZAÇÃO

Além dos benefícios e facilidades que a virtualização proporciona aos seus usuários como visto no Capítulo 2, os mesmos (os usuários) começaram a experimentar a virtualização como proposta para suprir outras necessidades e resolver outros tipos de problemas, como a segurança por exemplo. A segurança é um dos campos onde a virtualização pode ser aplicada, seja para isolar aplicações instáveis ou comprometidas, seja como solução de rápida recuperação de desastres, seja como ferramenta no auxílio de análises forenses ou até mesmo como uma solução de baixo custo para detecção de intrusão [13].

Com este novo campo em que a virtualização vem sendo empregada, tornou-se cada vez mais necessário que os *softwares* que fazem o compartilhamento do *hardware* físico fossem avaliados por uma entidade idônea. Esta avaliação ocorre para verificação do nível de segurança da estrutura do *software* testado.

Basicamente isto ocorreu por dois motivos: o primeiro é pela concentração do risco, ou seja, várias máquinas virtuais sendo executadas sobre um mesmo *hardware*; já o segundo, é que algumas empresas multinacionais e o governo de alguns países somente realizam a aquisição de produtos que sejam avaliados por essas entidades, como por exemplo, a *National Security Agency* (NSA), a qual faz parte do *U.S. Department of Defense* (Departamento de Defesa dos Estados Unidos). A NSA utiliza o *Common Criteria Evaluation and Validation Scheme* (CCEVS), que se trata de um conjunto de processos para a realização de validações em aplicativos e sistemas operacionais.

Baseada na necessidade da validação de segurança de seus produtos, a VMware Inc.[10], em 2006, fez com que dois de seus produtos fossem avaliados pela NSA, utilizando o CCEVS para tal. Os produtos que foram submetidos aos testes são o VMware ESX Server 2.5 [10] e o VMware *VirtualCenter Server* 1.0 [10]. Foram realizados vários testes para validar a segurança da solução de virtualização e gerenciamento do ambiente virtual formada pelo VMware ESX Server e o VMware *VirtualCenter Server* respectivamente.

Um exemplo da avaliação da segurança realizada é se algum usuário pode modificar ou deletar registros de auditoria com a finalidade de mascarar ou esconder um ataque ao sistema. Outro alvo da avaliação do CCEVS foi com relação ao isolamento das máquinas virtuais. Por exemplo, caso um atacante comprometa uma máquina virtual ou o servidor de virtualização, este atacante não deve ter acesso a recursos compartilhados ou não, entre as

máquinas virtuais (por exemplo, acesso a uma área de memória pertencente à determinada máquina virtual). O resultado dessa avaliação realizada em 2006 foi de que a solução avaliada recebeu o grau EAL2 (*Evaluation Assurance Level*) [14] [15]. O grau do EAL pode ir até o nível 7.

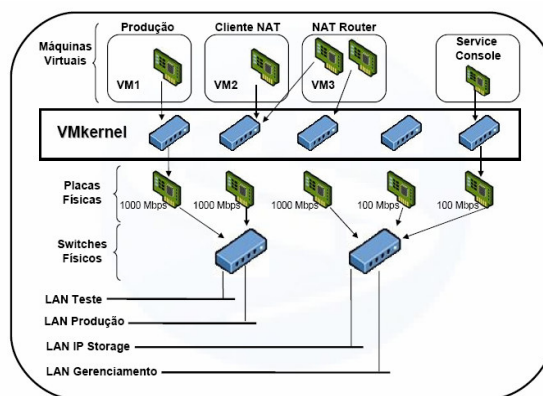
Atualmente, a VMware Inc. está submetendo as novas versões da solução de virtualização e gerenciamento do ambiente virtual (VMware ESX Server 3.0.1 e VMware VirtualCenter Server 2.0.1) a esses testes. Essas avaliações estão sendo conduzidas pelo instituto EWA-CANADA. Até o momento as novas versões da solução estão com o grau EAL4+ [16].

Na seção 3.1 deste capítulo será abordado como a virtualização pode ser utilizada para mitigar ameaças, sejam estas internas ou externas ao servidor de virtualização. As ameaças internas, ou *intra-host*, são mais difíceis de prover segurança com a utilização de ferramentas tradicionais, isto porque a comunicação dentro do servidor de virtualização tipicamente utiliza uma infra-estrutura virtual de rede e/ou outros canais de comunicação que não são vistos do “lado de fora” do servidor. Como resultado disso, equipamentos de *firewall* convencionais ou outras ferramentas de segurança que estão física e logicamente do “lado de fora” do servidor, não podem inspecionar ou controlar este tráfego que é transmitido via intra-estrutura virtual de rede. Isso faz com que a comunicação *intra-host* não seja monitorada, desprotegendo e expondo assim, as máquinas virtuais deste servidor [17].

Ao contrário das ameaças internas, as ameaças externas, ou *extra-host*, ao servidor de virtualização, podem ser mitigadas com técnicas aplicadas a qualquer tipo de ambiente, seja este virtual ou não. Pois o tráfego de rede das máquinas virtuais e do servidor de virtualização utiliza, por vezes, a infra-estrutura de rede externa ao mesmo, ou seja, a infra-estrutura física que todos acessam para transmitir dados (desde que tenham permissões). Nesse caso, *firewalls*, sistemas de detecção de intrusão e anti-vírus podem sim serem utilizados com sucesso na proteção da comunicação entre cliente/servidores ou servidor/servidor [17].

Na Figura 6 pode ser observado como uma máquina virtual pode ou não ter acesso a infra-estrutura de rede externa do servidor de virtualização. A máquina virtual Produção, por exemplo, possui uma interface de rede virtual. Essa interface de rede está conectada a um *switch* virtual, o qual é apresentado na linha do VMkernel. Para que essa máquina virtual tenha acesso à rede (LAN) Teste, o *switch* virtual que a máquina virtual utiliza foi “conectado” a interface física de rede do servidor de virtualização que está conectada a rede de Testes. Um exemplo de conexão *intra-host* pode ser observado nas máquinas virtuais

Cliente NAT e NAT Router. Onde essas máquinas virtuais possuem interfaces de redes conectadas a *switches* virtuais, mas esses *switches* virtuais não estão “conectados” a nenhuma interface física de rede do servidor. Por esse motivo, essas máquinas virtuais podem transmitir dados somente uma a outra.



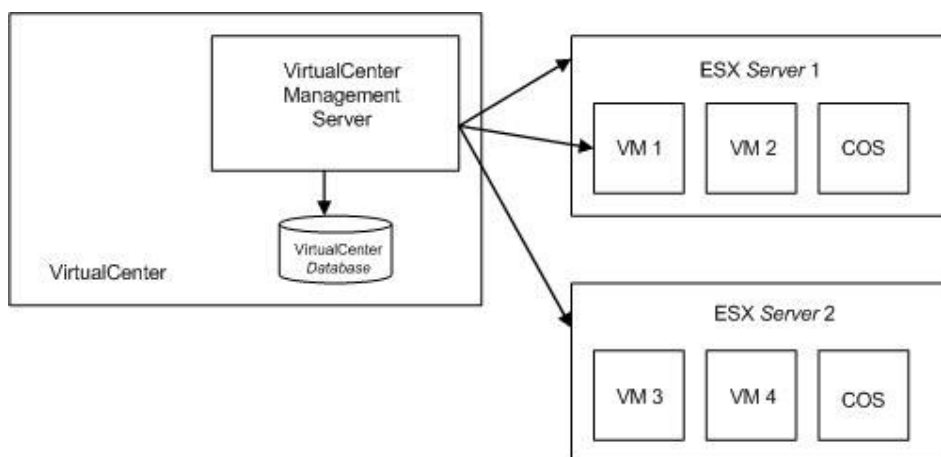
**Figura 6:** Exemplo de arquitetura virtual de rede  
**Fonte:** VMWARE INC., 2007.

### 3.1 SEGURANÇA DOS COMPONENTES BÁSICOS DO AMBIENTE VIRTUAL

O ambiente virtual é tradicionalmente formado por quatro componentes básicos, são eles: a) a *Service Console* ou COS; b) o *host* do VMware ESX Server; c) as máquinas virtuais; e d) o VMware *VirtualCenter Server*. Pelo fato desses quatro componentes serem de extrema importância para a garantia de segurança do ambiente virtual, serão descritas as medidas de segurança que devem ser tomadas para mitigar possíveis ameaças a esses quatro elementos.

Esses quatro componentes básicos são característicos da arquitetura do tipo I, como foi visto no Capítulo 2. Essa arquitetura foi escolhida em vista às suas funcionalidades, as quais não são pertinentes a arquitetura do tipo II. Além disso, a arquitetura do tipo I mostra-se mais estável se comparada a do tipo II. Logo, a arquitetura do tipo I é uma opção natural de escolha entre as empresas que buscam maior estabilidade para o ambiente virtual. Portanto, pelo fato do VMware ESX Server ter sido por muito tempo a única solução de virtualização que faz o uso da arquitetura do tipo I, o mesmo foi eleito como alvo de estudo e suporte a realização desse trabalho.

A Figura 7 mostra como ocorre a integração dos quatro componentes básicos do ambiente virtual.



**Figura 7:** Exemplo de integração dos componentes do ambiente virtual

**Fonte:** Adaptado de NATIONAL INFORMATION ASSURANCE PARTNERSHIP, 2007, p. 7.

A seguir serão descritas as medidas de segurança que devem ser aplicadas ao ambiente virtual. As medidas descritas abaixo não são configuradas por padrão durante a implementação de um ambiente virtual. Por isso, ao finalizar a implementação, deve-se realizar a configuração dessas medidas.

### 3.1.1 Proteção da *Service Console*

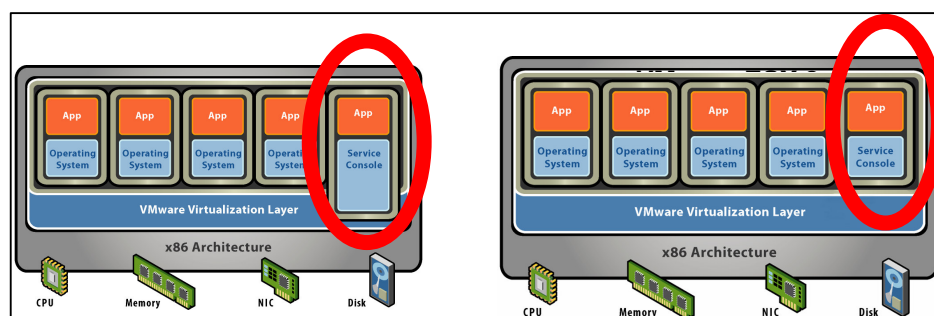
A primeira ação a ser tomada para elevar a segurança do ambiente virtual, é a proteção da *Service Console* (COS). Embora o *Virtual Machine Monitor* (VMM) esteja diretamente sobre o *hardware* físico do servidor de virtualização, faz-se necessária a existência de um componente fundamental, a COS.

A principal função da COS é controlar as requisições de acesso ao *hardware* físico. A COS também é responsável por realizar a chamada do VMM (chamado VMkernel no VMware ESX Server) para que este venha a entrar em execução quando o servidor é inicializado, fazendo assim com que o *hardware* físico possa ser particionado. Ou seja, a *Service Console* é uma console de gerenciamento do servidor de virtualização. É na *Service Console* onde se faz a priorização de acesso aos recursos de *hardware* físico. Caso a COS não existisse, os acessos aos recursos do servidor de virtualização seriam realizados de forma desordenada, podendo colocar assim as máquinas virtuais em um ambiente pouco estável.

Com a falta deste gerenciamento por parte da *Service Console*, uma máquina virtual poderia consumir todos os recursos de *hardware* disponíveis no servidor físico, podendo acarretar em uma falha geral no sistema e nas outras máquinas virtuais.

Embora a COS assemelhe-se visualmente a uma distribuição Linux, esta não pode ser administrada como se fosse uma distribuição padrão, pois a mesma possui outros comandos, sintaxes e ainda a adição de funcionalidades que não são pertinentes ao universo Linux. Atualmente, a última versão da COS do VMware ESX Server 3 é baseada na distribuição Red Hat Enterprise Linux 3.0 Update 6. O *kernel* desta distribuição sofreu diversas customizações com a finalidade de prover um ambiente estável, seguro e escalável para a execução e gerenciamento de máquinas virtuais. A Figura 8 mostra a relação entre as máquinas virtuais, suas aplicações, a camada de virtualização (VMware *Virtualization Layer*) e a *Service Console* nas versões VMware ESX Server 2.5 e 3.0.

Como pode ser observado na Figura 8 (no destaque circulado), houve uma alteração na arquitetura entre a camada de virtualização (VMware *Virtualization Layer*) e a *Service Console*. A *Service Console* é atualmente tratada com se fosse uma máquina virtual, ou seja, também compete por recursos de hardware. Essa alteração na arquitetura da COS com relação à camada de virtualização deve-se por algumas razões, uma delas é o desempenho, pois agora, na versão mais recente do VMware ESX Server (lado direito da figura), as interfaces de rede e as controladoras de armazenamento são gerenciadas diretamente pela camada de virtualização, e não mais pela *Service Console*.



**Figura 8:** Diferença na arquitetura da *Service Console* nas versões ESX 2 e ESX 3  
**Fonte:** VMWARE INC., 2007.

Pelo fato do VMware ESX Server ser uma versão altamente customizada de uma distribuição Linux, o mesmo é menos suscetível a vírus e outros problemas que geralmente afetam sistemas operacionais padrões. Entretanto, a *Service Console Server* não é totalmente imune a ataques. Por isso, medidas de segurança devem ser adotadas para dificultar ainda mais a ação das tentativas de ataques.

Para que o gerenciamento do servidor de virtualização e das máquinas virtuais possa ser realizado, faz-se necessário que a COS tenha um IP (*Internet Protocol*) configurado. Por este motivo, os softwares de gerenciamento de hardware (sistemas operacionais) que possuem um IP configurado em suas interfaces de rede estão propícios a se tornarem alvos das mais diversas tentativas de exploração de falhas.

Por padrão, algumas medidas de segurança já vêm configuradas e são utilizadas automaticamente. Aqui, pode-se citar o uso do protocolo SSL (*Security Socket Layer*) na comunicação entre VMware ESX Server e os clientes que o acessam, seja via web ou VI Client (*Virtual Infrastructure Client*). As conexões SSL utilizam o algoritmo AES de 256-bit para encriptar os blocos de dados. Já para a criptografia das chaves é utilizado o algoritmo RSA de 1024-bit. Outra medida tomada por padrão é o bloqueio de serviços que não utilizam qualquer método de criptografia de dados, como por exemplo, FTP (*File Transfer Protocol*) e Telnet.

As medidas que devem ser aplicadas à COS para garantir, ou aumentar, a segurança da mesma, são:

- Isolamento da Rede de Gerenciamento: a conectividade de rede para a COS é realizada através dos *switches* virtuais. Para aumentar a proteção a este componente crítico, faz-se necessário realizar o isolamento do mesmo utilizando um dos seguintes métodos:
  - Criação de uma VLAN separada para o gerenciamento da COS;
  - Configuração do acesso à COS através de um único virtual *switch*.

Ambos os métodos listados acima previnem que um atacante sem acesso a VLAN ou *virtual switch* da COS possam capturar o tráfego proveniente ou destinado a Service Console. Isso faz com que o atacante não consiga enviar qualquer pacote com destino a service console.

- Configuração do Firewall da COS: no caso do VMware ESX 3, o mesmo tem em sua estrutura um *firewall* (iptables) entre a conexão de rede e a COS. Por padrão, o *firewall* da COS é configurado com a opção mais alta de segurança, ou seja, todo o tráfego de entrada e saída, exceto para as portas 902, 80, 443 e 22, é bloqueado.

Pelo fato da maioria das portas serem bloqueadas na opção mais alta de segurança, após a instalação do VMware ESX Server, pode-se fazer a liberação de algumas destas (caso,



por exemplo, seja utilizado algum serviço na COS, como serviço de *backup*). A menos que seja necessário por alguma razão em particular, é extremamente recomendado que se deixe a configuração do *firewall* como alta.

- Uso do *VI Client* para administrar a COS: a melhor medida de segurança para evitar incidentes na COS é usá-la o menos possível no modo linha de comando. A maioria das configurações que podem ser realizadas através da linha de comando via SSH (*Secure Shell*), por exemplo, na COS, também devem ser realizadas utilizando o *VI Client* (modo gráfico). O acesso pelo *VI Client* pode ser realizado diretamente ao *host* ESX, utilizando a porta 902 TCP ou, melhor ainda, se for realizado através do VMware VirtualCenter Server. Além do *VI Client* se comunicar com o servidor ESX utilizando o protocolo SSL, o mesmo ainda utiliza uma API restrita, o que limita o que pode, ou não, ser feito. Com isso, minimiza-se a execução direta de comandos arbitrários.

Se for utilizado o *VI Client* em conjunto com o VMware *VirtualCenter* para acesso ao VMware ESX Server, tem-se ainda o benefício de que a autorização e autenticação seja realizada por um controlador de domínio, no caso o *Active Directory* da Microsoft, ao invés das contas de usuários locais da COS. Com a utilização de um controlador de domínio, os usuários e os papéis são armazenados em um banco de dados, facilitando assim a visualização das permissões de cada um. Além disto, o VMware *VirtualCenter* mantém histórico das ações realizadas pelos usuários, facilitando uma posterior auditoria.

- Utilizar um Serviço de Diretório para Autenticação: configurações avançadas e a pesquisa de problemas no *host* ESX podem necessitar de acesso privilegiado à COS. Para este tipo de circunstância, devem-se criar usuários e grupos locais na COS.

Esses usuários criados devem somente pertencer aos administradores que tem a responsabilidade de realizar a manutenção do ambiente virtual. Porém, esses usuários, apesar de serem em um número reduzido, necessitam que sejam criados em cada um dos servidores de virtualização. Dessa forma, isso pode representar um problema futuro na segurança, administração e gerenciamento destes usuários. Por isto, a utilização de um serviço de diretório é altamente recomendada. Assim, a partir de um único ponto os usuários são criados, gerenciados e autenticados.

- **Controle dos Privilégios do *Root* (superusuário):** o usuário *root* tem privilégios ilimitados na COS. A segurança desta conta de usuário é uma das medidas de segurança mais importantes para a proteção de todo o ambiente virtual. Por padrão, como dito anteriormente, todos os protocolos que não fazem utilização de criptografia, como FTP, Telnet e HTTP (*Hyper Transfer Text Protocol*), são desabilitados. O acesso remoto via SSH (*Secure Shell*) é habilitado, exceto para o usuário *root*.

Não é recomendado o acesso remoto ao usuário *root*, isto porque esta conta de usuário pode vir a ser comprometida em um ataque a rede para obtenção de sua senha. A melhor opção para acesso remoto a COS é fazer o *login* utilizando um usuário padrão, ou seja, uma conta de usuário que não tem poderes ilimitados e, após isto, utilizar o comando “*sudo*” para executar comandos privilegiados. O comando “*sudo*” faz com que somente o comando que se está executando tenha privilégios de *root*. Além disto, todos os comandos executados com o uso do “*sudo*” são gravados em log.

- **Limitar o acesso ao comando “*su*” (*Switch User*):** o acesso ao comando “*su*” deve ser estritamente de uso dos administradores do ambiente virtual, visto a sua grande capacidade de ocasionar um dano ao sistema caso seja usado erroneamente. Por padrão, somente usuários que estão no grupo *wheel* da COS têm permissão para executar o comando “*su*”. Se um usuário tentar utilizar o comando “*su*” para obter os privilégios de *root* e este usuário não estiver no grupo *wheel*, a tentativa irá falhar e este evento será registrado em log;
- **Estabelecer uma política de senhas para contas de usuários locais:** para qualquer usuário que é criado, a COS provê controles para as senhas que são criadas para estes usuários. Estes controles podem ser de dois tipos:
  - **Idade da Senha:** este controle permite configurar por quanto tempo a senha estará ativa antes que o usuário precise alterá-la. Isto faz com que, caso um atacante venha a comprometer a senha de algum usuário, o mesmo não poderá continuar acessando a COS indefinidamente;
  - **Complexidade da Senha:** este controle faz com que os usuários escolham senhas que sejam difíceis de serem adivinhadas por um ataque de força bruta ou ataque de dicionário.

- Limitar os *softwares* e serviços que são executados na Service Console: softwares adicionais podem ser instalados e executados na COS, como, por exemplo, agentes de gerenciamento e agentes de backup. Os serviços que podem ser executados incluem, por exemplo, NIS (*Network Information Service*), SNMP (*Simple Network Management Protocol*) ou HTTPS (*HyperText Transfer Protocol Secure*). Embora a finalidade do uso destes softwares seja importante, os mesmos podem conter brechas de segurança que podem vir a comprometer a Service Console. Para o funcionamento destes serviços, é necessário que portas específicas sejam abertas, fazendo com que esses serviços tornem-se mais um ponto de exploração de falhas;
- Não realizar o gerenciamento da *Service Console* como se fosse uma distribuição Linux: a *Service Console* é baseada na distribuição Linux Red Hat. Esta foi cuidadosamente customizada para prover exatamente as funcionalidades necessárias para se comunicar e gerenciar o VMKernel. Por isto, qualquer tipo de software adicional não deve ser instalado, a não ser que este esteja na lista de compatibilidade da COS.

Apesar de a COS utilizar o RPM (*Red Hat Package Manager*) como gerenciador de pacotes, os pacotes instalados na Service Console têm seus códigos modificados especificamente para a mesma.

Outro fato relevante é quanto à aplicação de correções. Nunca deve ser aplicada uma correção que tenha sido liberada pela Red Hat ou por terceiros (Apache, OpenSSH, etc...). As correções que devem ser aplicadas na COS devem ser liberadas pela própria VMware.

- Estabelecer e Manter a Integridade do Sistema de Arquivos: a *Service Console* contém vários arquivos onde estão armazenadas suas configurações. São eles:

/etc/profile

/etc/ssh/sshd\_config

/etc/pam.d/system\_auth

/etc/ntp

/etc/ntp.conf

/etc/passwd

/etc/group

/etc/sudoers

/etc/shadow

Além destes, arquivos que estão dentro do diretório /etc/vmware são os que armazenam as configurações do VMKernel.

Todos estes arquivos devem ser monitorados com o fim de garantir a integridade e alteração não autorizada dos mesmos. A integridade destes arquivos pode ser monitorada fazendo-se o uso de ferramentas como *tripewire* ou *sha1sum* (esta última é presente na COS). Backups regulares devem ser realizados nos arquivos listados acima.

- Manutenção de Logs: fazer o registro de ações ou eventos em arquivos específicos para esse fim (arquivos de log) é uma boa prática para manutenção de qualquer sistema. Manter o registro de atividades incomuns no sistema pode até fazer um pré-anúncio de um ataque, caso os mesmos sejam visualizados regularmente. Esses arquivos também devem ser analisados após o sistema ter sido comprometido, pois com eles será possível aprender como prevenir ataques futuros.

### 3.1.2 Proteção do *host* VMware ESX Server

As medidas que devem ser aplicadas ao *host* ESX Server para garantir, ou aumentar, a segurança do mesmo, são:

- Nomenclatura clara das redes virtuais: nomear todas as redes virtuais apropriadamente para a prevenção de confusões ou comprometimento da segurança. Essa nomenclatura previne que o administrador cometa um erro ao adicionar uma máquina virtual a uma rede virtual que ela não possa ter acesso, evitando assim o vazamento de informações sensíveis;
- Não criar um *PortGroup* padrão: durante a instalação do ESX Server, existe a possibilidade da criação de um *portgroup* para as máquinas virtuais. Entretanto, ao se fazer a criação do *portgroup* padrão para as máquinas virtuais este é criado na mesma interface de rede que a COS irá utilizar. Com a criação deste *portgroup* padrão, as máquinas virtuais podem, em algum momento, capturar o tráfego decifrado que é endereçado à COS;

- Usar uma interface de rede isolada e dedicada para o VMotion e iSCSI: pelo fato das informações que são trocadas entre os servidores ESX quando ocorre a movimentação on-line das máquinas virtuais (VMotion) não estarem criptografadas, informações sensíveis podem ser capturadas nessa rede utilizada para o VMotion. Por isso, é extremamente recomendado que a rede utilizada para VMotion seja isolada das demais redes. Existe ainda a possibilidade da utilização da criptografia SSL via hardware. Para o tráfego iSCSI não existe criptografia disponível, portanto a rede de iSCSI também deve ser isolada;
- Não utilizar interfaces de rede em modo promíscuo: no ESX Server existe a possibilidade de que uma interface de rede virtual possa ser colocada em modo promíscuo. O modo promíscuo pode ser habilitado tanto nos *switches* virtuais que estão associados a interfaces de rede físicas (vmnic), como nos *switches* virtuais que não estão associados a nenhuma interface de rede física (vmnet). Quando o modo promíscuo é habilitado a uma vmnic, todas as máquinas virtuais que estão conectadas a este *virtual switch* estão propensas a terem seus tráfegos capturados através da rede física ou virtual. Porém, quando o modo promíscuo é habilitado a uma vmnet, somente as máquinas virtuais conectadas a este *switch* (vmnet) podem ter seus tráfegos capturados;
- Proteção contra alteração do endereço MAC (*Media Access Control*): cada adaptador de rede virtual das máquinas virtuais tem seu próprio endereço MAC. Esse endereço é criado quando se realiza a criação de uma nova máquina virtual. Entretanto, através do sistema operacional que está instalado dentro da máquina virtual é possível fazer a troca do endereço MAC por outro qualquer. Quando se faz esta alteração de MAC, a máquina virtual começa a receber também o tráfego que é destinado a este novo MAC. Com isto, esta máquina virtual pode enviar pacotes de dados à rede com um endereço MAC de origem forjado. Para que este tipo de ataque não aconteça, pode-se desabilitar a possibilidade de alteração de MAC dos *switches* virtuais nos perfis de segurança do ESX Server. As configurações a serem desabilitadas são: troca de endereço MAC e falsificação de transmissões;
- Configuração de acesso ao *storage* externo (*zoning*): o *zoning* provê controle de acesso a rede da área de armazenamento externo. No *zoning* é definido quais *hosts bus adapters* (HBA) podem se conectar a determinadas áreas do *storage* externo. Quando o *zoning* é configurado, interfaces HBA que não fazem parte do *zoning* não

conseguem enxergar áreas destinadas a outros adaptadores. Portanto, a configuração de *zoning* deve ser realizada com o máximo de restrições possíveis, isto para que outros servidores não tenham acesso a áreas restritas do *storage* externo;

- Proteção contra ocupação total do sistema de arquivos: quando se está fazendo a instalação do *ESX Server*, a opção recomendada de particionamento de disco é a padrão. Caso seja escolhida a forma de particionamento manual, é fundamental a criação de partições */home*, */tmp* e */var/log*. Isto porque geralmente estes são os diretórios que apresentam um crescimento rápido, fazendo com que a partição raiz do sistema seja ocupada totalmente. Se a partição raiz for ocupada totalmente, vários problemas podem ser ocasionados, como por exemplo, causar a queda de todas as máquinas virtuais do servidor *ESX*.

### 3.1.3 Proteção das Máquinas Virtuais

As próximas medidas devem ser tomadas para garantir um maior nível de segurança para as máquinas virtuais. A maioria dessas medidas é aplicada também a servidores físicos. Isso porque os sistemas operacionais que são instalados nas máquinas virtuais são os mesmos que são instalados em servidores físicos, ou seja, não sofrem nenhum tipo de alteração em seus códigos pelo fato de resistirem sobre uma plataforma de virtualização.

- Desabilitar serviços desnecessários: o simples fato de desabilitar serviços que não são necessários reduz o número de alvos que podem ser atacados. As medidas são:
  - Desabilitar serviços não utilizados pelo sistema operacional da máquina virtual;
  - Desconectar dispositivos físicos que não são utilizados (ex.: *cd/dvd*, *disquete* e *portas USB*);
  - Em sistemas *Linux*, *BSD* e *Solaris*, não instalar o sistema *X Windows*;
  - Desabilitar as operações de copiar e colar entre a máquina virtual e a console remota (*VI Client*).
- Uso de máquinas virtuais modelo: a utilização de máquinas virtuais modelo é de grande ajuda. Assim, ao se realizar a customização de um modelo, todas as outras

máquinas virtuais criadas a partir deste modelo terão as mesmas características de segurança;

- Prevenir que as máquinas virtuais tomem o controle dos recursos físicos: alguns serviços de virtualização, como o VMware ESX *Server*, possuem a capacidade de controle de alocação de recursos físicos para as máquinas virtuais. Isso quer dizer que é possível fazer um ajuste fino nas configurações de acesso ao hardware físico por parte das máquinas virtuais. Ou seja, é uma boa prática, enclausurar as máquinas virtuais dentro dos requisitos necessários para o bom desempenho de sua função. Assim, é possível evitar que uma máquina virtual cause uma negação de serviço ao consumir demasiadamente todos os recursos disponíveis de hardware, fazendo com que as outras máquinas virtuais venham a ter seu funcionamento ou desempenho comprometidos;
- Limitar o fluxo de dados entre as máquinas virtuais e o *host* ESX: as máquinas virtuais podem salvar diversas informações em arquivos de log (vmware.log). Além de cada máquina virtual ter seus próprios arquivos de log, estes estão localizados no mesmo diretório onde são armazenados os discos virtuais.

As máquinas virtuais podem ser configuradas para salvar um grande volume de informações dentro destes arquivos de log. Com isso, intencionalmente ou inadvertidamente, estes arquivos podem ganhar proporções (tamanhos) muito grandes. Com o passar do tempo, estes arquivos ao serem manipulados pelo ESX *Server* podem consumir muitos recursos de hardware físico, como por exemplo, espaço de armazenamento de discos virtuais. Caso isso venha a acontecer, pode-se causar uma negação de serviço, fazendo assim, com que o servidor pare de responder. Para conter esse problema, pode-se configurar o ESX *Server* para que este apague os arquivos de log mais antigos ou quando atingirem um determinado tamanho.

- Isolar a rede das máquinas virtuais: embora o hardware virtual de uma máquina virtual seja isolado das demais, as máquinas virtuais estão normalmente conectadas a redes compartilhadas. Uma máquina virtual, ou grupo de máquinas virtuais, conectadas a uma rede comum comunicam-se através dessa rede, consequentemente essas máquinas virtuais podem se tornar alvos de ataques de outra máquina virtual que pertence à mesma rede. Por isto, a segmentação de rede diminui o risco de vários ataques acontecerem, como por exemplo, o ARP (*Address Resolution Protocol*) *spoofing*. Além disto, a segmentação de redes virtuais facilita

a auditoria, isto porque mostra claramente a qual (ais) rede(s) as máquinas virtuais estão conectadas. Esta segmentação pode ser realizada de duas maneiras, são elas:

- Segmentação física, ou seja, cada segmento de rede diferente na organização possui uma interface de rede física específica para a mesma;
  - Segmentação lógica, ou seja, em uma única interface de rede física são criadas VLANs para cada segmento de rede diferente na organização.
- Reduzir o uso do *VI Client* para acesso direto ao *VMware ESX Server*: quando utiliza-se o *VI Client* para acessar a uma determinada máquina virtual, tem-se acesso a console desta. A console nada mais é do que se enxergar o que um monitor instalado em uma máquina física estaria mostrando.

Entretanto, o *VI Client* proporciona um gerenciamento avançado da máquina virtual, podendo assim desconectar dispositivos dessa máquina virtual, os quais sem a VM (*Virtual Machine*) pode apresentar uma falha. Além disto, ao serem abertas várias seções com o *VI Client* a um servidor ESX, este necessita obter mais recursos físicos para o gerenciamento dos usuários, o que pode degradar o desempenho do mesmo. Ao invés de se utilizar o *VI Client* para acessar a uma máquina virtual, ferramentas nativas ao sistema operacional da VM podem ser utilizados, com o *terminal services* e o SSH.

### 3.1.4 Proteção do VMware *VirtualCenter Server*

Por último e não menos importante para a garantia de um nível de segurança adequado para a infra-estrutura virtual, será descrito quais medidas devem ser adotadas para a proteção do *VirtualCenter Server*.

O *VirtualCenter Server* provê uma forma de realizar o gerenciamento e controle de todo o ambiente virtual de um único ponto. Com o *VirtualCenter Server* torna-se possível a utilização de ferramentas que podem diminuir o tempo de parada das máquinas virtuais. O mesmo é um aplicativo que deve ser instalado (segundo recomendações do manual) em um servidor que tenha a Microsoft *Windows Server* como sistema operacional, e um banco de dados. Este banco de dados pode ser tanto a Microsoft SQL Server como o Oracle. As primeiras recomendações de segurança para o sistema operacional onde o VMware



*VirtualCenter Server* é instalado, são recomendações padrão a qualquer sistema operacional, como: a) instalação de antivírus, b) instalação de *anti-spyware*, c) instalação de um sistema de detecção de intrusão e d) aplicação dos *patches* de segurança recomendados pelo desenvolvedor do sistema operacional.

As medidas adicionais são:

- Configuração do Microsoft *Windows Server* com o nível de segurança apropriado: pelo fato do *VirtualCenter* ser instalado sobre um sistema operacional, no caso o Microsoft *Windows*, torna-se necessário proteger o sistema operacional contra vulnerabilidades e ataques;
- Limitar o Acesso Administrativo: o serviço do *VirtualCenter* é executado com um usuário que tem privilégios de administrador local. Para limitar o acesso administrativo é recomendado evitar o uso da conta de administrador local. Para tal, é aconselhado a criação de um usuário específico para executar o serviço do *VirtualCenter*. Esse usuário deve ter os privilégios limitados às suas funções;
- Limitar a conectividade de rede ao *VirtualCenter*: as únicas redes que o *VirtualCenter* deve acessar são as redes onde se encontram os servidores ESX e as redes onde estão instalados os clientes que fazem acesso ao *VirtualCenter Server*. Deve-se evitar a colocação do *VirtualCenter* em qualquer outra rede de onde o mesmo não será acessado, como a DMZ (*DeMilitarized Zone*) ou a rede de armazenamento por exemplo.

Além disto, existe outra medida para limitar a conectividade, que é a utilização de um *firewall*. Nesse *firewall* devem ser bloqueadas todas as portas que não serão utilizadas e filtrar os endereços que podem ter acesso via rede ao *VirtualCenter*. Esse bloqueio deve ser feito com cuidado, pois o bloqueio de uma porta ou protocolo necessário para o funcionamento de alguma funcionalidade, pode fazer com que o *VirtualCenter* venha a apresentar algum erro.

- Configurações de segurança para o Banco de Dados que o *VirtualCenter* fará uso: um servidor de banco de dados, para uso pelo *VirtualCenter*, deve ser instalado em uma máquina diferente de onde o *VirtualCenter* será instalado. Devem ser configuradas cuidadosamente as permissões de acesso dos usuários ao banco de dados. Estas permissões devem ser as mais restritas possíveis. Como o *VirtualCenter* pode utilizar tanto o Microsoft *SQL Server* como o Oracle para armazenar as informações de gerenciamento do ambiente virtual, os mesmos devem

ser configurados seguindo as recomendações de segurança de seus desenvolvedores;

- Habilitar o uso seguro da criptografia baseada em certificados: todas as versões dos produtos da VMware utilizam o padrão X.509 de certificados para criptografar as informações trocadas entre cliente e servidor.

Entretanto, nas versões mais recentes do *VirtualCenter*, o cliente não faz a verificação da autenticidade do certificado do servidor apresentado durante a fase de *hand-shake* do protocolo SSL. Isto faz com que os clientes estejam vulneráveis ao ataque *man-in-the-middle*. Porém, os *patches* de segurança lançados para o *VirtualCenter* corrigem este problema para clientes Windows.

Durante a instalação dos produtos da VMware, certificados auto-assinados são gerados. Entretanto, os certificados gerados pelo *VirtualCenter*, incluindo os da versão 2.0.1 *Patch 1*, não devem ser utilizados, pois os mesmos contêm bugs de programação. Ao contrário disso, os certificados gerados durante a instalação dos servidores VMware ESX *Server* devem sim ser utilizados. Para isto, é necessário que os usuários que irão conectar-se diretamente aos servidores ESX aceitem estes certificados auto-assinados pelos servidores ESX. Para ambientes que necessitem de uma segurança ainda mais forte, a VMware recomenda que certificados gerados e assinados por Autoridades Certificadora sejam utilizados.

- Utilização de papéis do *VirtualCenter*: uma das principais características do *VirtualCenter* é a possibilidade da utilização, ou criação, de papéis para a definição das permissões dos usuários. Estes papéis permitem determinar com uma grande granularidade quais as permissões que cada usuário terá sobre cada objeto (*datacenter*, máquina virtual, *clusters*, etc...) do *VirtualCenter*. Além dos papéis padrão, é possível a criação de papéis customizados de acordo com cada necessidade.

### 3.2 FERRAMENTAS DISPONÍVEIS PARA O AMBIENTE VIRTUAL

Ao longo desse trabalho, descreveu-se como a virtualização vem alterando o cenário atual dos ambientes computacionais. Dentre as alterações descritas está o uso da virtualização

como suporte a segurança das máquinas virtuais. A utilização da virtualização para prover, ou aumentar, a segurança dos serviços críticos ao negócio das organizações é possível tendo em vista de que determinadas funcionalidades estão disponíveis somente ao ambiente virtual. Esse suporte à segurança pode ser apresentado como, por exemplo, o aumento da disponibilidade desses serviços críticos.

Após a descrição das medidas de segurança que devem ser adotadas nos quatro componentes fundamentais de um ambiente virtualizado (COS, *host* ESX, máquinas virtuais e *VirtualCenter*), será descrito como a integração destes quatro componentes junto com outras quatro ferramentas podem ajudar a manter o ambiente virtual o mais seguro possível.

Ao fazer-se uso de toda a infra-estrutura virtual que a VMware disponibiliza, torna-se possível a utilização de quatro ferramentas que ajudam a garantir, por exemplo, alta-disponibilidade, rápida recuperação, balanceamento de carga e integridade ao ambiente virtual. A seguir será descrito cada funcionalidade dessas quatro ferramentas e como elas integram-se. São elas: a) VMotion, b) HA (*High Availability*), c) DRS (*Distributed Resource Scheduler*) e d) *Consolidated Backup*.

### 3.2.1 Movimentação de Máquinas Virtuais *On-line*

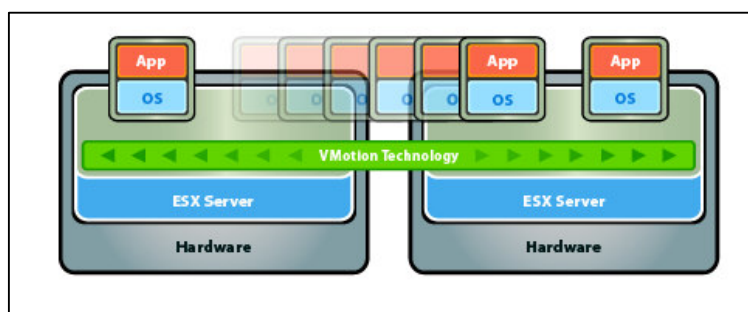
A tecnologia VMotion possibilita a migração *on-line* das máquinas virtuais em execução entre servidores VMware ESX. Ou seja, possibilita que as máquinas virtuais sejam movimentadas entre servidores físicos sem a necessidade de desligamento das mesmas, mantendo assim, a disponibilidade dos serviços executados pelas máquinas virtuais.

Além disso, o VMotion é o responsável por manter os dados íntegros durante essa transferência (seja da memória, seja do disco virtual da máquina virtual). Essa movimentação *on-line* somente pode ser realizada por causa de três princípios:

- 1) Todo o estado de uma máquina virtual é encapsulado por um conjunto de arquivos mantidos em uma área de armazenamento externa e compartilhada, como a SAN (*Storage Area Network*), por exemplo. Além disso, o sistema de arquivos VMFS (*Virtual Machine File System*), o qual é utilizado para armazenar os discos virtuais das máquinas virtuais pode ser acesso por vários servidores VMware ESX ao mesmo tempo de forma concorrente;

- 2) A memória ativa da máquina virtual é rapidamente transferida entre os servidores VMware ESX via uma rede de alta velocidade, normalmente, através de uma conexão *gigabit ethernet*. Assim, é possível que todo o conteúdo de memória da máquina virtual possa ser enviado para o servidor de destino. Todo esse processo de transferência é transparente para os usuários que utilizam os serviços disponibilizados por estas máquinas virtuais. Isto porque o VMotion mantém em um log todas as transações realizadas durante a transferência do conteúdo de memória da máquina virtual entre os servidores. Após o término da cópia de todo o conteúdo de memória e do estado atual da máquina virtual é que o VMotion suspende a máquina virtual origem e aplica as alterações de memória que estavam no arquivo de log da máquina virtual origem na máquina virtual destino. Todo o processo descrito acima costuma ocorrer em menos de 1 minuto em uma rede *gigabit ethernet*;
- 3) Pelo fato das redes utilizadas pela máquina virtual também serem virtualizadas pelo VMkernel do VMware ESX, isso faz com que se preserve a identidade e conectividade das máquinas virtuais durante o processo de migração. Para isso o VMotion também faz o gerenciamento do endereço MAC virtual. Uma vez que a máquina virtual foi migrada de servidor, o VMotion realiza um teste de *ping* no *switch* virtual para certificar-se de que a máquina virtual está respondendo pelo mesmo MAC.

A Figura 9 mostra o funcionamento do VMware VMotion, onde está ilustrado a



transferência de uma máquina virtual (ligada) entre dois servidores VMware ESX Server.

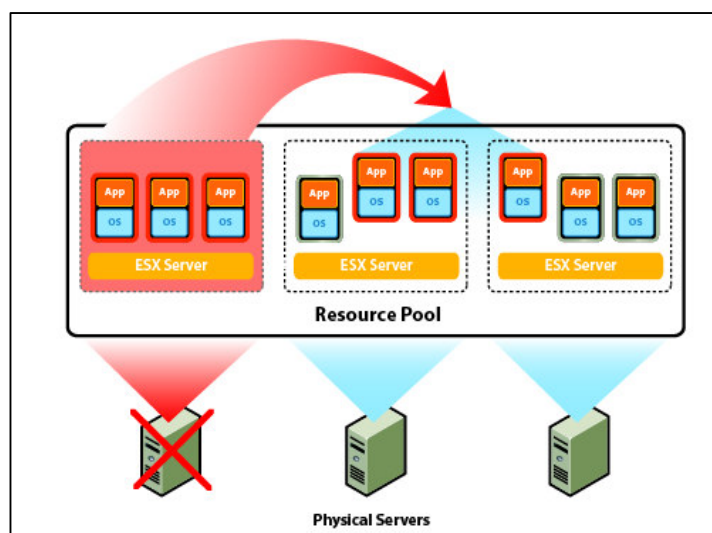
**Figura 9:** Exemplo do funcionamento da ferramenta VMotion

**Fonte:** VMWARE INC., 2007.

### 3.2.2 Alta-disponibilidade das Máquinas Virtuais

O VMware *High Availability* provê uma solução simples e a um baixo custo de alta-disponibilidade para as aplicações que são executadas pelas máquinas virtuais. Na ocorrência de uma falha em um servidor VMware ESX, as máquinas virtuais afetadas por essa falha são automaticamente re-iniciadas em outro servidor VMware ESX. Isso é possível, pois o VMware HA faz a monitoração contínua de todos os servidores como um conjunto de recursos para a detecção da falha. O agente que é executado em cada um dos servidores VMware ESX mantém um *heartbeat* com os outros servidores do conjunto de recursos. No caso de perda deste *heartbeat*, o VMware HA verifica as máquinas virtuais afetadas e inicia o processo de re-inicialização dessas máquinas virtuais nos outros servidores ativos que formam o conjunto de recursos.

A Figura 10 exemplifica a falha de um dos servidores físicos que compõe o pool de recursos. Conseqüentemente, as máquinas virtuais que estavam em execução nesse servidor, irão também parar de funcionar. Com isso, as máquinas virtuais desse servidor são iniciadas



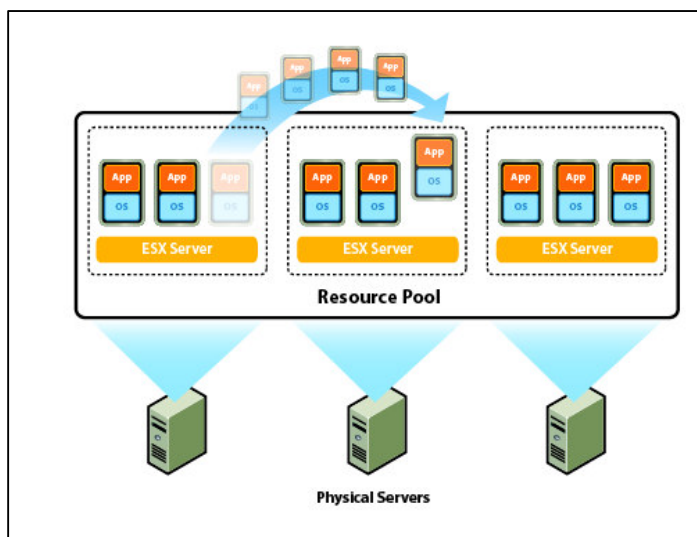
nos outros dois servidores disponíveis no pool de recursos.

**Figura 10:** Exemplo do funcionamento da ferramenta HA  
**Fonte:** VMWARE INC., 2007.

### 3.2.3 Balanceamento de carga entre os servidores VMware ESX Server

O VMware *Distributed Resource Scheduler* dinamicamente realoca e faz o balanceamento de carga entre os servidores VMware ESX que formam o conjunto de recursos lógicos. O DRS realiza a monitoração da utilização dos recursos físicos dos servidores e das máquinas virtuais em execução. Com isso, o DRS pode fazer a realocação dessas máquinas virtuais entre servidores VMware ESX que tenham recursos ociosos, promovendo assim o balanceamento de carga entre todo o conjunto de recursos. O balanceamento de carga utiliza o VMotion para que as máquinas virtuais possam ser transferidas de um servidor para outro sem a interrupção de seus serviços.

A Figura 11 mostra o exemplo de uma máquina virtual, que ao necessitar de mais recursos computacionais é transferida para outro servidor VMware ESX de forma *on-line*. Para decidir o servidor de destino da máquina virtual, o DRS realiza a verificação do servidor mais ocioso que possa receber a máquina virtual.



**Figura 11:** Exemplo do funcionamento da ferramenta DRS

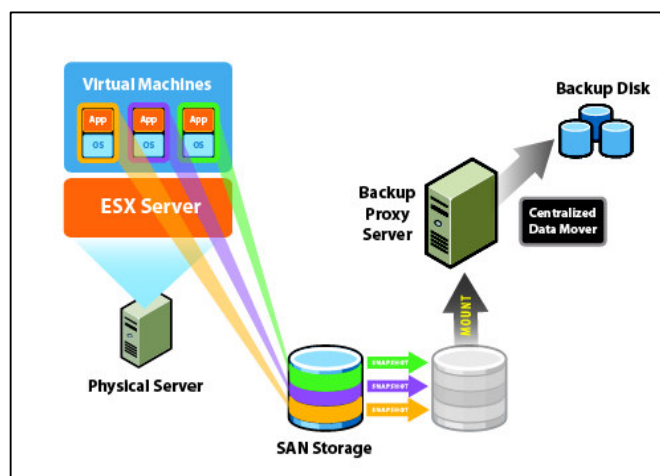
**Fonte:** VMWARE INC., 2007.

### 3.2.4 Backup do Ambiente Virtual

O VMware *Consolidated Backup* funciona como um centralizador de *backup* das máquinas virtuais. Ou seja, o *Consolidated Backup* é um conjunto de *drivers* e *scripts* que

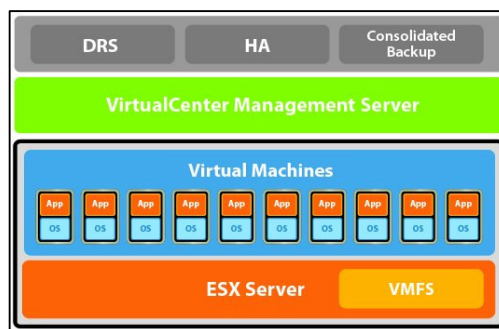
realizam o *backup* via *LAN-free* das máquinas virtuais que são executadas nos servidores VMware ESX. Esses *drivers* e *scripts* fazem com que o *Backup Proxy Server* possa acessar os volumes VMFS que estão na área de armazenamento externo e realizar um *snapshot* (cópia) das máquinas virtuais em funcionamento.

A Figura 12 exemplifica a ação do *Consolidated Backup* de realizar a cópia on-line das máquinas virtuais que estão no *storage* externo (aqui exemplificado como *SAN Storage*) e enviar essa cópia para a área de backup (*Backup Disk*).



**Figura 12:** Exemplo do funcionamento da ferramenta *Consolidated Backup*  
**Fonte:** VMWARE INC., 2007.

A Figura 13 exemplifica como os componentes DRS, HA e *Consolidated Backup* integram-se ao ambiente virtual, mais especificamente ao VMware *VirtualCenter*. Onde se tem as máquinas virtuais que estão armazenadas no VMFS e instanciadas sobre os servidores que executam o VMware ESX. Por sua vez, o VMware *VirtualCenter* realiza todo o gerenciamento dos servidores VMware ESX, das máquinas virtuais e, também, do DRS, HA e *Consolidated Backup*.



**Figura 13:** Integração das funcionalidades DRS, HA e CB ao ambiente virtual.  
**Fonte:** VMWARE INC., 2007.

## 4 DISPONIBILIDADE, CONFIDENCIALIDADE E INTEGRIDADE

Neste capítulo, ao passo que foram descritas no capítulo anterior as quatro ferramentas complementares para a segurança da infra-estrutura virtual, essas, juntamente com as medidas de segurança que devem ser aplicadas no ambiente virtual, serão caracterizadas de acordo com as características de segurança que cada uma dessas ferramentas e medidas provém. Isso para que seja possível o aumento ou garantia da disponibilidade, confidencialidade e integridade, seja das máquinas virtuais, seja da *Service Console*, seja do ambiente virtual como um todo.

### 4.1 DISPONIBILIDADE

De acordo com a NBR17799, a definição de disponibilidade é a garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário [18].

Pelo fato da concentração de risco ser inerente a virtualização, a parada de um servidor físico (programada ou não), acaba por afetar várias máquinas virtuais. Dentre essas, algumas máquinas virtuais que não podem estar indisponíveis para acesso por um período prolongado.

Para que a disponibilidade das máquinas virtuais seja garantida, tem-se a disposição dos administradores do ambiente virtual algumas ferramentas e boas práticas que fazem com que o período de indisponibilidade das máquinas virtuais seja o menor possível. Aqui são apresentados quais são essas ferramentas e boas práticas que devem ser aplicadas ao ambiente virtual. São elas:

- Controlar os privilégios do usuário *root*: a *Service Console* exerce papel de fundamental importância para o gerenciamento das máquinas virtuais e dos recursos físicos que são controlados e distribuídos pela mesma às máquinas virtuais. Para a administração da *Service Console*, faz-se necessária a utilização de um usuário com privilégios ilimitados ao sistema (super-usuário). Esse usuário, tipicamente nomeado de “*root*”, tem o poder de realizar qualquer tipo de operação na COS, seja esta operação para prover algum tipo de melhoria ao sistema, seja



para ocasionar uma parada total das máquinas virtuais. Por padrão o usuário “*root*” tem acesso total ao sistema, isto é, possui total controle sobre o estado da COS, das máquinas virtuais e do hardware que está sendo virtualizado para as VM's. Tendo esse total controle, uma vez que o usuário *root* foi comprometido, um atacante pode promover uma parada completa, tanto do serviço de virtualização, como pontualmente de cada máquina virtual. Essa parada do sistema de virtualização e das máquinas virtuais pode acontecer executando-se comandos nativos ao VMware ESX Server. O comprometimento dos recursos de hardware pode vir a acontecer injetando-se, por exemplo, um código malicioso. Por esses motivos é que se faz o controle dos privilégios que o usuário “*root*” terá ao realizar a administração da Service Console. Outras boas práticas ajudam a prevenir que o usuário “*root*” venha a ser comprometido, como, por exemplo, a utilização de criptografia sempre que realizar-se o acesso remoto à COS, ou ainda a troca periódica da senha do usuário “*root*”;

- Prevenção contra o controle total dos recursos físicos por parte de uma máquina virtual: uma das avaliações realizadas pela NSA é com relação ao isolamento existente entre as máquinas virtuais. Por exemplo, a garantia de que uma área em memória, mesmo que compartilhada, não sofrerá manipulações de outra máquina virtual qualquer. Mesmo a NSA tendo avaliado esse isolamento, não só com relação à memória, existem formas de colocar limites quanto à utilização do hardware físico por parte das máquinas virtuais, em outras palavras, é possível a colocação da máquina virtual em uma “jaula”. Esta “jaula” pode ser criada nativamente com ferramentas disponíveis no VMware ESX Server. Com essas ferramentas pode-se, por exemplo, fazer a definição de limites da quantidade de memória RAM que a máquina virtual terá disponível para seu uso. Além deste limite da quantidade de utilização de cada recurso de hardware físico disponível, pode-se ainda realizar a priorização de acesso a determinado recurso, ou seja, é permitido que uma máquina virtual, sempre que necessitar de algum recurso físico (como processamento), seja sempre a primeira da fila. Com isso, toda vez que esta determinada máquina virtual precisar fazer uso do processador, a mesma terá prioridade maior com relação às outras máquinas virtuais. Essa priorização pode ser aplicada a uma máquina virtual em específico ou a um grupo de servidores VMware ESX. Seja de forma manual ou automatizada, as máquinas virtuais necessitam voltar a seu funcionamento o mais

rápido possível. Com este cenário, e para minimizar o tempo de parada de uma ou mais máquinas virtuais, pode-se fazer uso de duas tecnologias descritas anteriormente, o VMotion e o HA;

- VMotion: o VMotion é normalmente utilizado quando tem-se paradas programadas a serem realizadas no servidor VMware ESX. No momento em que se define que um servidor necessita ser desligado, por exemplo, para adição de mais recursos físicos (como memória ou processadores), o simples fato de desligar este servidor faz com que várias máquinas virtuais fiquem indisponíveis para acesso. Assim, faz-se uso do VMotion para movimentar as máquinas virtuais em funcionamento para outro servidor disponível, assim não mais tornando indisponível os serviços daquela máquina virtual;
- HA: já quando ocorre uma parada não programada, causada por uma falha de hardware, por exemplo, é utilizado o HA. O HA, ao verificar que ocorreu a perda de um servidor VMware ESX, faz a reinicialização automática das máquinas virtuais afetadas, ou seja, que estavam instanciadas sobre aquele servidor, em um outro servidor disponível. Com a utilização do HA, o tempo de parada das máquinas virtuais é igual ao tempo de inicialização do sistema operacional que está instalado na máquina virtual. O processo de reinicialização das máquinas virtuais é totalmente automatizado e controlado, ou seja, caso determinadas máquinas virtuais não sejam de criticidade alta, ou têm um tempo permitido de indisponibilidade maior, essas podem permanecer desligadas. Isso é comum quando o(s) outro(s) servidor(es) não possuem recursos de hardware suficientes para que todas as máquinas virtuais que foram afetadas pela falha do servidor VMware ESX sejam iniciadas. O controle da escolha de qual servidor em que a máquina virtual será reinicializada é feito quando se utiliza o HA em conjunto com o DRS. Realizando-se uma conta simples, pode-se chegar com o HA a um tempo de disponibilidade que supere os 99,99%. Isso levando-se em conta que uma máquina virtual não demore mais do que 10 minutos para que o sistema operacional que a mesma comporta tenha sido carregado completamente, e, que essa máquina virtual venha a ser comprometida pela falha de um servidor VMware ESX somente uma vez em um ano;

## 4.2 CONFIDENCIALIDADE

A NBR 17799 definiu confidencialidade como a garantia de que a informação é acessível somente por pessoas autorizadas a terem acesso [18]. Nessa definição, não é dito explicitamente como será realizado o controle de que a informação seja acessada somente por usuários que tenham permissões para tal. Mesmo sem essa definição de como dados sensíveis devem ser guardados com o fim de evitar ao máximo que os mesmos sejam divulgados, uma das formas de garantir a confidencialidade das informações é a utilização da criptografia.

Com este entendimento sobre a definição de confidencialidade, existem algumas boas práticas que podem e devem ser utilizadas com a finalidade de minimizar que um usuário, sem permissão, tenha acesso a dados sensíveis. São estas boas práticas:

- Estabelecimento de políticas de senhas para usuários locais: o fato de exigir senhas complexas na criação dos usuários, ou o tempo de vida que cada senha terá, faz com que a adivinhação de senhas por parte do atacante não seja uma tarefa tão trivial. Ou seja, quando não se realiza a exigência de senhas complexas, ou com o tempo de vida prolongado, pode-se permitir com que um atacante tenha acesso a dados considerados sensíveis pela organização. Essas políticas podem ser aplicadas tanto para usuários criados nas COS quanto para usuários criados no controlador de domínio;
- Utilização de uma interface de rede dedicada para VMotion e iSCSI: as máquinas virtuais, quando são transferidas através da tecnologia VMotion, não sofrem nenhum tipo de tratamento quanto a sua confidencialidade. Isso quer dizer que ao se transferir uma máquina virtual entre dois servidores distintos, ao se capturar o tráfego de VMotion, pode-se fazer a interpretação imediata dos dados transferidos. Além do Vmotion, quando se utiliza o iSCSI como forma de acesso a uma área de armazenamento externo, os dados que são trocados entre o servidor VMware ESX e esta área de armazenamento, não passam por nenhum tratamento quanto a confidencialidade. Ou seja, os dados trafegam em “aberto”. Por isso, recomenda-se a segmentação tanto da rede de Vmotion quanto da rede de iSCSI;
- Não utilizar interfaces de rede em modo promíscuo: com a utilização de uma interface ou de um *switch* virtual em modo promíscuo torna-se possível a captura dos dados que trafegam pela infra-estrutura virtual de rede. Uma vez que esses

dados não passam por nenhum algoritmo de criptografia, os mesmos podem ser visualizados sem problema algum;

- Proteção do MAC contra falsificação: ao realizar a proteção de que as máquinas virtuais não possam realizar a alteração de seus respectivos endereços MAC, está garantindo-se de que nenhuma máquina virtual, ao alterar o seu endereço MAC irá receber ou enviar dados para a rede local fazendo-se passar por outra máquina virtual. Com essa proteção, os dados destinados aos endereços MAC originais, serão recebidos pelas máquinas virtuais que devem ter acesso a esses dados;
- Configuração apropriada da SAN (*Storage Area Network*): a correta configuração de *zoning* da área de armazenamento de dados externo (SAN) faz com que servidores não tenham acesso à área de dados de outros servidores. Em virtude de uma configuração mal realizada em um *storage* externo, um atacante que tenha comprometido um servidor, seja ele físico ou virtual, pode acessar essa área de armazenamento de dados externo e realizar a leitura, ou até mesmo deletar arquivos contidos nesse espaço;
- Utilização dos papéis para usuários: se determinadas informações são pertinentes a usuários específicos, convém realizar a definição de papéis, ou seja, privilégios, que cada usuário terá ao realizar o *logon*, seja no servidor ESX, seja no servidor *VirtualCenter*. A definição deve ser realizada de forma mais restritiva possível. Isso garante que os usuários tenham acesso somente às informações que os mesmos devem acessar para realizar suas tarefas. Por exemplo, usuários que devem ter acesso somente às máquinas virtuais, não devem ter acesso, mesmo que somente de leitura, a arquivos de configuração do ambiente virtual, tão pouco aos arquivos de outros usuários, arquivos esses que podem ser os discos virtuais das máquinas virtuais;
- Utilização de criptografia: a utilização da criptografia é uma das formas mais antigas para que uma determinada informação seja lida e interpretada somente por pessoas autorizadas. Em um ambiente computacional utiliza-se a criptografia para o mesmo fim, fazer com que pessoas que não devem ter acesso a informação não consigam interpretá-la corretamente. Na infra-estrutura virtual faz-se o uso da criptografia em vários pontos sensíveis de troca de informações. Seja no acesso a COS via linha de comando, ou no acesso ao servidor ESX via navegador, é possível a utilização de protocolos que protejam qualquer tipo de informação trocada entre

cliente e servidor. Pode-se citar o SSH (*Secure Shell*) como uma forma de acesso criptografado a COS. Outra forma de realizar o acesso seguro ao ambiente virtual é a utilização de certificados digitais. Esses certificados digitais podem ser utilizados tanto para acesso a interface *web* do servidor ESX, quanto para acesso via *Virtual Infrastructure Client*;

- Segmentação de redes: outra forma de manter a informação em domínios restritos é a utilização de VLAN's. Uma determinada máquina virtual, conectada a um *virtual switch* que pertença a uma determinada VLAN, pode somente enviar e receber dados de outros servidores, ou máquinas virtuais que façam parte da mesma VLAN. Nessa mesma linha de segmentação de redes, pode ser utilizado o conceito de *internal network*. Ou seja, um *switch virtual* que tem este tipo de configuração não está acessível por outros componentes de rede, a não ser que esses outros componentes também estejam conectados a esse *virtual switch*. Esse tipo de configuração é normalmente empregado quando se tem uma máquina virtual, servidor de banco de dados, por exemplo, que deve ser acessada exclusivamente por outra máquina virtual. Então cria-se uma rede interna entre o servidor de banco de dados a máquina virtual em questão. Pode-se fazer uma analogia a rede física como se fossem conectados dois servidores físicos via um cabo de rede *crossover*.

#### 4.3 INTEGRIDADE

Já a integridade é definida pela NBR17799 como a salvaguarda da exatidão e totalidade da informação e dos métodos de processamento [18].

Nesta seção será tratado como garantir integridade para os arquivos da COS. Estes arquivos podem ser de vários tipos, como binários, arquivos de configuração, e os discos das máquinas virtuais (arquivos.vmdk). Não será abordado como garantir integridade aos dados que estão dentro das máquinas virtuais, ou seja, arquivos que estão dentro dos discos virtuais, ao visto que isso é pertinente ao tipo de sistema operacional que é executado dentro de cada máquina virtual.

As medidas para manter a integridade dos arquivos são:

- Manter a integridade do sistema de arquivos: identificar se um ou mais arquivos sofreram qualquer tipo de alteração em seu conteúdo, seja essa alteração permitida ou não, é de grande importância para, por exemplo, a realização de auditorias ao ambiente computacional. Arquivos de logs podem ser alterados para mascarar um ataque por exemplo. Já arquivos binários ou os arquivos de configurações do sistema, podem sofrer alterações para que o ambiente apresente um comportamento fora do padrão ou até mesmo para que seja aberta uma *backdoor* no servidor. Comumente realiza-se a verificação da integridade dos arquivos que estão dentro dos diretórios `/bin`, `/var/log` e `/etc/vmware`. O primeiro diretório citado é onde estão os arquivos binários do VMware ESX Server. Já no segundo diretório é onde se encontram os arquivos de log do sistema, importante quando se realiza uma auditoria ou a busca de problemas. Por fim, no terceiro diretório citado, `/etc/vmware`, é onde se encontram todos os arquivos de configurações do ambiente virtual. A alteração indevida de algum arquivo que se encontra dentro do diretório `/etc/vmware` pode comprometer o funcionamento do ambiente virtual. Outros arquivos que devem ser verificados são os discos virtuais das máquinas virtuais, ou seja, os arquivos com extensão `.vmdk`. Ao manter-se um controle sobre esses arquivos, tem-se a certeza de que nenhum disco virtual foi colocado no lugar dos originais. Esses novos discos virtuais podem ser trocados por outros que tenham um conteúdo alterado. Para a verificação da integridade dos arquivos citados, seja os que estão dentro do `/bin`, `/var/log`, `/etc/vmware` ou dos discos virtuais, pode-se utilizar ferramentas nativas ao VMware ESX, como por exemplo o *sha1sum*. Outra ferramenta que pode ser instalada na *Service Console* é o *tripwire*;
- Utilização de uma ferramenta de backup apropriada para os discos virtuais: o ato de realizar o backup de arquivos importantes é uma prática que deve ser aplicada a qualquer ambiente, seja este um ambiente virtual ou não. Porém, só a realização do backup de arquivos não garante nem a integridade dos arquivos que são “backupeados”, tão pouco a rápida recuperação de uma máquina virtual. Além do backup periódico dos discos virtuais das máquinas virtuais, testes de recuperação do ambiente devem ser realizados frequentemente. Manter a integridade dos discos das máquinas virtuais é uma tarefa nem sempre realizada com sucesso pelas ferramentas de backup para arquivos comuns. Pois ao manipular um arquivo `.vmdk`

(disco virtual) além de estar se tratando de arquivos com 50, 60 ou até mesmo arquivos com mais de 100GBytes, estes arquivos possuem um sistema de arquivos cujo a máquina virtual utiliza para armazenar seus dados. Por isso a escolha de uma solução de backup apropriada que possa compreender a diferença entre um arquivo comum do sistema operacional e um arquivo de disco virtual. Ao utilizar ferramentas nativas ao VMware ESX, como vcbMounter e vcbRestore, para a realização do backup e da recuperação de máquinas virtuais, está se garantindo que os dados das máquinas virtuais não sejam corrompidos. Isso porque esses dois comandos, vcbMounter e vcbRestore, interagem com sistema de arquivos onde estão armazenados os discos virtuais das máquinas virtuais (VMFS) para que o VMFS faça o *unlock* e o *lock* dos discos virtuais nos momentos em que a máquina virtual terá os seus discos virtuais manipulados;

- Configuração de *zoning*: a correta configuração de *zoning* na rede de armazenamento faz com que servidores não tenham acesso aos dados de outros servidores. Ou seja, caso dois servidores tenham recebido permissão para acessar a mesma área de armazenamento externo por engano, ao momento em que esses servidores tentarem realizar uma escrita de dados nessa área, essa área pode vir a ser corrompida. Por outro lado, o acesso simultâneo de dois servidores a mesma área pode não corromper os dados ali contidos, mas sim possibilitar que um dos servidores obtenha esses dados, dados que por muitas vezes podem ser dados sensíveis para a organização.

## 5 ESTUDO DE CASO

Esta etapa do trabalho compreende o planejamento da virtualização do ambiente de servidores da organização Fundação CEEE. Com base nas informações levantadas do ambiente atual da empresa, nas necessidades atuais de infra-estrutura e segurança, e nas melhores práticas de segurança para implementação de um ambiente virtual, será proposto um projeto de virtualização dos servidores mais críticos ao negócio da Fundação CEEE.

Com base em entrevistas com os administradores do ambiente computacional da Fundação CEEE serão avaliados quais os servidores que necessitam de maiores cuidados com relação à segurança. Nesta entrevista será analisada também a arquitetura de rede atual. Uma análise importante a ser feita é a da carga de trabalho atual dos servidores. Porém, não faz parte deste trabalho nem a descrição da metodologia da avaliação desta carga de trabalho, nem a descrição da metodologia de dimensionamento dos recursos de hardware dos servidores onde será instalado o VMware ESX *Server*. Embora esta avaliação da carga e dimensionamento dos recursos seja de suma importância para o bom desempenho, escalabilidade e estabilidade do ambiente virtual.

### 5.1 INFORMAÇÕES DA EMPRESA

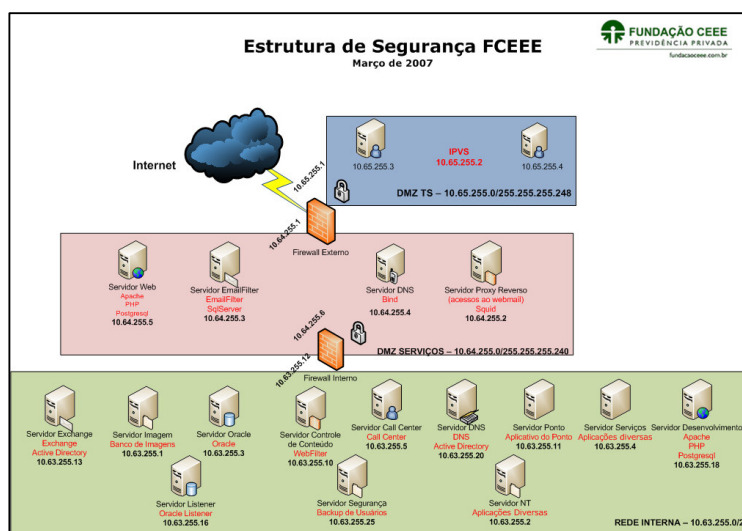
A empresa Fundação CEEE de Seguridade Social atua no ramo de fundo de pensão dos funcionários da CEEE, RGE, AES e CGTE e tem sua sede principal localizada na cidade de Porto Alegre – Rio Grande do Sul. Atualmente a empresa possui um quadro de 90 funcionários sediados em Porto Alegre.

A escolha da empresa foi tomada considerando-se o atual ambiente computacional. Uma das considerações foi que a empresa atualmente não conta com nenhum serviço de virtualização de servidores. Outro ponto decisivo foi a falta de alta-disponibilidade para serviços críticos, como o servidor de banco de dados, servidor *listener* (serviço de consultas a empréstimos via *web*) e o servidor controlador de domínio.

Atualmente a Fundação CEEE conta com 19 servidores físicos que provêm os mais diversos serviços a seus usuários. Além disso, como pode ser observada na Figura 14, a



arquitetura de rede está dividida em quatro partes: a) Internet, b) DMZ TS, c) DMZ SERVIÇOS e d) Rede Interna.



**Figura 14:** Ambiente computacional atual da Fundação CEEE

**Fonte:** FUNDAÇÃO CEEE, 2007, p. 3.

## 5.2 CENÁRIO ATUAL

Atualmente no ambiente computacional da Fundação CEEE existem 19 servidores como dito anteriormente. A configuração desses servidores pode ser observada abaixo:

Modelo: DELL PowerEdge 1950  
 Processador: Pentium 4 3.0 GHz  
 Memória RAM: 2G  
 Armazenamento Interno: 2 discos SCSI 73 G (RAID1)  
 Rede: 1 x 3COM (10/100Mbit)  
 Serviços: Páginas de Internet

Modelo: DELL PowerEdge 1900  
 Processador: Pentium 4 3.0 GHz  
 Memória RAM: 1G  
 Armazenamento Interno: 2 discos SCSI 73 G (RAID1)  
 Rede: 1 x 3COM (10/100Mbit)  
 Serviços: Filtro de correio eletrônico

Modelo: DELL PowerEdge 830  
Processador: Pentium 3 700 MHz  
Memória RAM: 2G  
Armazenamento Interno: 1 disco SCSI 73 G (RAID1)  
Rede: 1 x 3COM (10/100Mbit)  
Serviços: Resolução de Nomes

Modelo: DELL PowerEdge 840  
Processador: Pentium 4 1.8 GHz  
Memória RAM: 2G  
Armazenamento Interno: 2 discos SCSI 73 G (RAID0)  
Rede: 1 x 3COM (10/100/1000Mbit)  
Serviços: Proxy

Modelo: DELL PowerEdge 6600  
Processador: 2 x Pentium 4 3.0 GHz  
Memória RAM: 2G  
Armazenamento Interno: 4 discos SCSI 73 G  
Rede: 1 x 3COM (10/100/1000Mbit)  
Serviços: Correio Eletrônico

Modelo: DELL PowerEdge 1900  
Processador: Xeon 1.6 GHz  
Memória RAM: 2G  
Armazenamento Interno: 2 discos SCSI 73 G (RAID1)  
Rede: 1 x 3COM (10/100Mbit)  
Serviços: Imagens (Banco de Imagens)

Modelo: DELL PowerEdge 6600  
Processador: Pentium 4 3.0 GHz  
Memória RAM: 4G  
Armazenamento Interno: 2 discos SCSI 73 G  
Rede: 1 x 3COM (10/100/1000Mbit)  
Serviços: Banco de Dados Produção

Modelo: DELL PowerEdge  
Processador: Pentium 4 3.0 GHz  
Memória RAM: 1G  
Armazenamento Interno: 2 discos SCSI 73 G (RAID1)  
Rede: 1 x 3COM (10/100Mbit)  
Serviços: Controle de Conteúdo de Internet

Modelo: Desktop  
Processador: Pentium 3 1 GHz  
Memória RAM: 512M  
Armazenamento Interno: 1 disco PATA 20G  
Rede: 1 x 3COM (10/100Mbit)  
Serviços: Central de Atendimento Telefônico

Modelo: DELL PowerEdge  
Processador: Pentium 4 3.0 GHz  
Memória RAM: 2G  
Armazenamento Interno: 2 discos SCSI 73 G (RAID1)  
Rede: 1 x 3COM (10/100/1000Mbit)  
Serviços: Resolução de Nomes e Controlador de Domínio.

Modelo: DELL PowerEdge  
Processador: Pentium 4 3.0 GHz  
Memória RAM: 1G  
Armazenamento Interno: 2 discos SCSI 73 G (RAID1)  
Rede: 1 x 3COM (10/100/1000Mbit)  
Serviços: Desenvolvimento de Aplicações

Modelo: DELL PowerEdge 830  
Processador: Pentium 4 3.0 GHz  
Memória RAM: 512M  
Armazenamento Interno: 2 discos SCSI 73 G (RAID1)  
Rede: 1 x 3COM (10/100/1000Mbit)  
Serviços: Anti-vírus e Anti-SPAM

Modelo: DELL PowerEdge 830  
Processador: Pentium 4 3.0 GHz  
Memória RAM: 1.5G  
Armazenamento Interno: 2 discos SCSI 73 G (RAID1)  
Rede: 1 x 3COM (10/100Mbit)  
Serviços: Arquivos

Modelo: Desktop  
Processador: Pentium 4 3.0 GHz  
Memória RAM: 2G  
Armazenamento Interno: 1 disco PATA 80 G  
Rede: 1 x Intel (10/100Mbit)  
Serviços: Ponto Eletrônico

Modelo: DELL PowerEdge  
 Processador: Pentium 4 3.0 GHz  
 Memória RAM: 2G  
 Armazenamento Interno: 2 discos SCSI 73 G (RAID1)  
 Rede: 1 x 3COM (10/100Mbit)  
 Serviços: Backup

Modelo: DELL PowerEdge  
 Processador: Pentium 4 3.0 GHz  
 Memória RAM: 2G  
 Armazenamento Interno: 2 discos SCSI 73 G (RAID1)  
 Rede: 1 x Intel (10/100Mbit)  
 Serviços: Banco de dados Desenvolvimento

Modelo: DELL PowerEdge  
 Processador: Pentium 4 3.0 GHz  
 Memória RAM: 2G  
 Armazenamento Interno: 2 discos SCSI 73 G (RAID1)  
 Rede: 1 x 3COM (10/100Mbit)  
 Serviços: Serviço de Terminal (WTS)

Modelo: DELL PowerEdge  
 Processador: Pentium 4 3.0 GHz  
 Memória RAM: 2G  
 Armazenamento Interno: 2 discos SCSI 73 G (RAID1)  
 Rede: 1 x 3COM (10/100/1000Mbit)  
 Serviços: Impressão

Modelo: DELL PowerEdge  
 Processador: Pentium 4 3.0 GHz  
 Memória RAM: 2G  
 Armazenamento Interno: 2 discos SCSI 73 G (RAID1)  
 Rede: 1 x Realtek (10/100Mbit)  
 Serviços: Aplicações Diversas

Apesar desses 19 servidores apresentarem algum tipo de redundância em um ou mais de seus componentes de hardware, como por exemplo, arranjo de discos (RAID) ou fontes redundantes, caso algum servidor venha a apresentar uma falha de um componente, de qualquer que seja esse componente, tem-se de esperar ao menos quatro dias úteis para que a compra seja efetuada. Em meio a esse período de compra, caso o servidor não tivesse redundância nesse componente que falhou, o servidor ficaria indisponível para acessos.

Além disso, atualmente nenhum dos servidores de produção conta com um servidor de contingência, ou seja, caso algum dos servidores de produção venha a apresentar uma falha

geral, é necessária primeiramente a descoberta de um hardware dentro do parque computacional da Fundação CEEE que tenha os mesmos recursos de hardware do servidor que apresentou a falha. Após isso, realiza-se a instalação completa dos aplicativos que estavam instalados no servidor, e de seus pré-requisitos, para a volta de seu funcionamento. Por vezes essa tarefa entre obter um novo hardware, instalar os aplicativos necessários para a restauração do serviço e recuperação dos dados do *backup* pode levar pelo menos 24 horas. Se estas 24 horas forem divididas em horas comerciais, está falando-se em pelo menos três dias de trabalho até que o serviço esteja novamente disponível para os usuários.

### 5.3 NECESSIDADES ATUAIS DA EMPRESA

Como resultado do levantamento das atuais necessidades da empresa realizado através de reuniões com os responsáveis pela manutenção dos servidores e da rede da Fundação CEEE, obteve-se:

- Necessidade de criação de um ambiente isolado e controlado para área de desenvolvimento;
- Necessidade de alta-disponibilidade e rápida recuperação para servidores considerados críticos para a organização (*Listner*, banco de dados, e-mails e arquivos);
- Necessidade da colocação no *site* de backup de um servidor que contenha as imagens virtualizadas dos servidores críticos;
- Necessidade da criação de políticas de backup para os dados dos servidores;
- Necessidade de melhor aproveitamento de hardware;
- Necessidade de redução do espaço físico ocupado pelos servidores no *datacenter*;
- Segmentação da rede de servidores;
- Necessidade de gerenciamento centralizado dos servidores.

Com base nas necessidades atuais da Fundação CEEE, será elaborado um projeto que contemplará a implementação de um ambiente virtual para que os problemas atuais possam ser resolvidos. Para que o projeto possa ser viabilizado, será necessária a aquisição de novos

hardwares, com o fim de propiciar um ambiente seguro e que possa suportar um crescimento de 35% no ano. Os componentes envolvidos no projeto de implementação do ambiente virtual da Fundação CEEE são:

- Dois servidores com a seguinte configuração onde será instalado o VMware ESX *Server*:
  - 2 Processadores Quad Core 2.0+ Ghz;
  - 16 GB de memória RAM;
  - 6 Interfaces de rede gigabit *ethernet*;
  - 2 Controladoras HBA para conexão com o *storage* externo;
  - 1 Controladora Disco que suporte a criação de RAID;
  - 2 Discos SAS 73Gb (RAID1).
- Um servidor com a seguinte configuração onde será instalado o VMware VirtualCenter *Server*:
  - 1 Processador 3.0+ Ghz;
  - 2 GB de memória RAM;
  - 1 Interface de rede *gigabit ethernet*;
  - 1 Controladora Disco que suporte a criação de RAID;
  - 2 Discos SAS 73Gb (RAID1).
- Um servidor com a seguinte configuração onde será instalado o VMware *Consolidated Backup*:
  - 1 Processador 3.0+ Ghz;
  - 2 GB de memória RAM;
  - 1 Interface de rede *gigabit ethernet*;
  - 2 Controladoras HBA para conexão com o *storage* externo;
  - 1 Controladora Disco que suporte a criação de RAID;
  - 2 Discos SAS 73Gb (RAID1).
- Uma área de armazenamento externo com capacidade para receber os dados de todos dos discos de todos os atuais servidores. Essa área foi estimada em 1.5TB.

Além da aquisição de hardware, faz-se também necessária a aquisição de softwares. Esses softwares serão os responsáveis por prover todos os recursos imprescindíveis para sanar as necessidades citadas anteriormente. A lista de software é composta por:

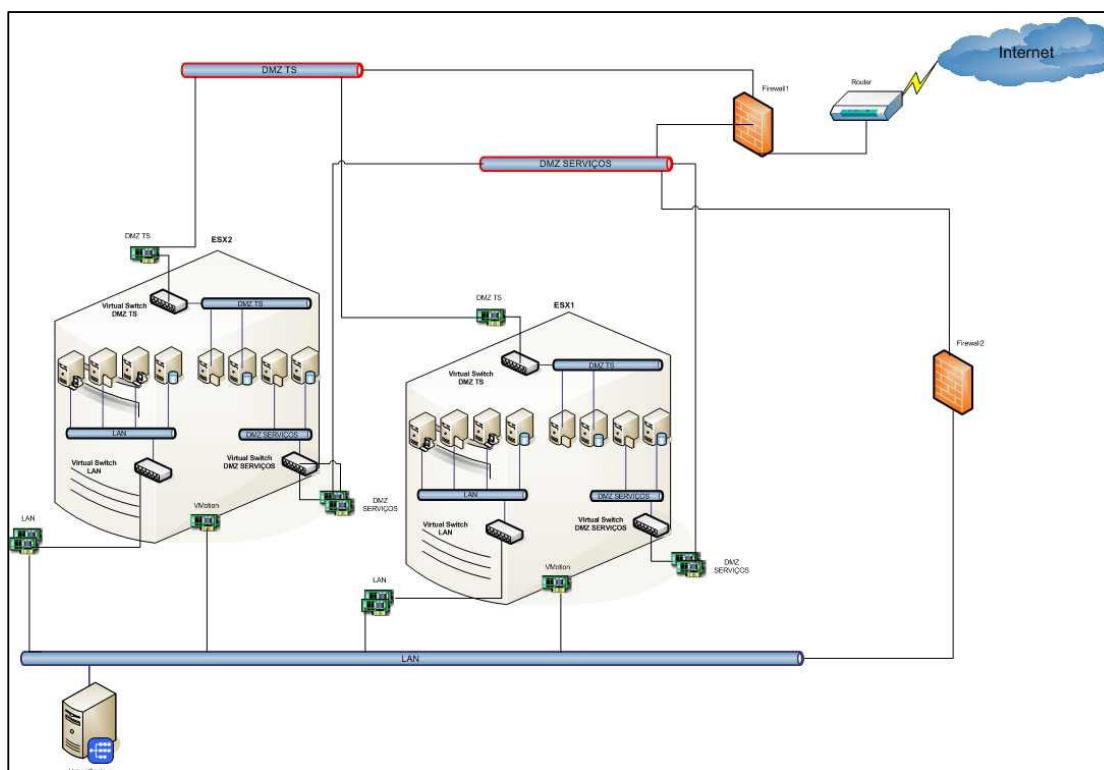
- Duas licenças do software *VMware ESX Server Enterprise Edition*;
  - Obs.: A licença do software *VMware ESX Server Enterprise Edition* contempla as seguintes funcionalidades: a) HA, b) DRS, c) VMotion e d) *Consolidated Backup*;
- Uma licença do software *VMware VirtualCenter Server*;

A Figura 15 apresenta o novo ambiente já virtualizado da Fundação CEEE. Apesar dos dois *firewalls* que a empresa utiliza atualmente poderem ser virtualizados, a mesma optou em não virtualizar nesse momento visto a pouca experiência com a nova tecnologia.

Para que as necessidades de disponibilidade, integridade e confidencialidade do ambiente projetado fossem supridas, foram utilizados os seguintes recursos e medidas de segurança:

- Recursos:
  - VMotion;
  - HA;
  - DRS;
  - *Consolidated Backup*;
  - Agrupamento de interfaces de rede;
  - *Multipath* para acesso ao *storage* externo.
- Medidas de Segurança:
  - Controle dos privilégios do usuário root;
  - Utilização de uma interface de rede dedicada para VMotion e iSCSI;
  - Proteção do MAC contra falsificação;
  - Configuração apropriada da SAN (*Storage Area Network*);
  - Utilização de criptografia;
  - Segmentação de redes (*Switches* Virtuais dedicados a sua determinada função);

- Utilização de uma ferramenta de *backup* apropriada para os discos virtuais.



**Figura 15:** Ambiente computacional projetado para a Fundação CEEE

**Fonte:** Elaborado pelo autor.

Conforme proposto no Capítulo 3 desse trabalho, no qual foram relacionadas as melhores práticas de segurança que devem ser aplicadas ao ambiente virtual e, também, como a tecnologia da virtualização pode ajudar a garantir um ou mais dos pilares fundamentais da segurança da informação, obteve-se como resultado o projeto apresentado neste capítulo. Com esse projeto, espera-se, assim que implementado, que as indisponibilidades causadas seja por um ataque, vírus, falha de hardware ou software, sejam mitigadas ao máximo, fazendo com que o ambiente virtual possa continuar em funcionamento mesmo na ocorrência das mesmas.



## 6 CONCLUSÃO

Desde a concepção da virtualização em meados de 1960, onde começou a pesquisar-se sobre uma maneira de melhor aproveitar o hardware, a mesma vem sendo utilizada para os mais diversos fins. Embora as idéias inovadoras sobre a possibilidade da criação de ambientes isolados não tenham tido aceitação e fomentação, tanto por parte de empresas privadas como na área acadêmica, hoje tem-se visto a utilização em larga escala de ambientes virtuais. Essa utilização vai desde ambientes de treinamento e desenvolvimento, até os ambientes de homologação e produção das organizações.

Tendo em vista essa larga utilização da virtualização nos mais diversos ambientes computacionais, as organizações começaram a migrar todos os seus ambientes tradicionais (um servidor físico por aplicação), para um ambiente virtual. Com isso, serviços e sistemas considerados críticos aos processos de negócios das empresas, começaram a ter o suporte da virtualização para o seu funcionamento. Mesmo residindo sobre um ambiente virtual, esses serviços e sistemas devem ser protegidos contra as ameaças alheias. Foi nessa necessidade de manter um ambiente virtual o mais seguro possível, e, ainda tirar os benefícios que a virtualização dispõe para prover (ou aumentar) a segurança desse ambiente que as empresas começaram a migrar seus ambientes tradicionais para as plataformas de virtualização. Esses motivos formaram o ponto chave para realização desse trabalho.

No Capítulo 2 foi descrito desde a origem das máquinas virtuais, passando pelos tipos de arquiteturas, vantagens, desvantagens e, terminando com os ambientes em que a virtualização pode ser empregada. Já no Capítulo 3 foram descritas as medidas de segurança que se deve aplicar a um ambiente virtual para que este seja o mais seguro possível. Nesse capítulo, também se fez menção ao fato da virtualização ter se tornado uma ferramenta de segurança a favor da disponibilidade de ambientes de missão crítica. O Capítulo 4 trouxe como as medidas de segurança e funcionalidades propiciadas pela virtualização podem ajudar a manter o ambiente disponível, íntegro e confidencial. Todo esse estudo das boas práticas de segurança para a virtualização pôde ser aplicado em um projeto para a organização Fundação CEEE, descrito no Capítulo 5. Nesse estudo de caso fez-se um levantamento do ambiente computacional atual, bem como das necessidades de segurança que a organização passava. Com a aplicação das medidas de segurança e funcionalidades da virtualização propostas no Capítulo 4, pode-se projetar um ambiente seguro, estável e escalável para a Fundação CEEE.

Ainda pode-se citar como trabalho futuro, após a implementação do ambiente proposto, uma entrevista com os administradores de rede e servidores da Fundação CEEE, com o objetivo de avaliar se as necessidades de segurança foram atendidas pelo projeto. Além disso, um estudo minucioso sobre o funcionamento do isolamento entre as máquinas virtuais poderá ser realizado. Com esse estudo pretende-se realizar a validação do isolamento entre os recursos de hardware virtual que são entregues para as máquinas virtuais. Onde o servidor de virtualização será submetido a constantes injeções de falha em memória.

## REFERÊNCIAS

- [1] FEDOROVA, Alexandra. *Making the Most Out of OS Virtual Machine Technology*. Disponível em: <<http://www.eecs.harvard.edu/~fedorova/papers/253final-fedorova.pdf>>. Acesso em: 25 nov. 2006.
- [2] **REVISTA INFOEXAME**. São Paulo, p. 76, dez. 2006.
- [3] INFO CORPORATE. **Máquinas Virtuais chegarão a 4 milhões em 2009**. Disponível em: <[http://info.abril.com.br/corporate/noticias/noticia\\_231932.shtml](http://info.abril.com.br/corporate/noticias/noticia_231932.shtml)>. Acesso: 18 maio 2007.
- [4] WRIGHT, Chris. *Virtually Linux – virtualization techniques in Linux*. Disponível em: <<http://www.finux.org/Reprints/Reprint-Wright-OLS2004.pdf>>. Acesso em: 26 nov. 2006.
- [5] WHITAKER, Andrew. *Building Robust Systems with Virtual Machine Monitors*. Disponível em: <<http://www.cs.washington.edu/homes/andrew/pubs.html>>. Acesso em: 26 nov. 2006.
- [6] KELEM, N., FEIERTAG, R. *A Separation Model for Virtual Machine Monitors. Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy*. Washington, p. 78-86, 1991.
- [7] ROBIN, John S.; IRVINE, Cynthia E. *Analysis of the Intel Pentium's Ability to Support a Secure Virtual Machine Monitor*. Disponível em: <[www.cs.nps.navy.mil/people/faculty/irvine/publications/2000/VMM-usenix00-0611.pdf](http://www.cs.nps.navy.mil/people/faculty/irvine/publications/2000/VMM-usenix00-0611.pdf)>. Acesso em: 05 jan. 2007.
- [8] MCEWAN, William. *Virtual Machine Technology and Their Application In The Delivery of ICT*. In: *ANNUAL NATIONAL ADVISORY COMMITTEE ON COMPUTING QUALIFICATIONS (NACCQ)*, 15., 2002, *Hamilton. Proceedings*. Hamilton: NACCQ, 2002. p. 55-62. Disponível em: <<http://site.tekotago.ac.nz/staticdata/papers02/papers/mcewan55.pdf>>. Acesso em: 2 set. 2006.
- [9] **BOCHS: The Open Source IA-32 Emulation Project**. Disponível em: <<http://bochs.sourceforge.net/>>. Acesso em: 18 jun. 2007.
- [10] **VMWARE INC**. Disponível em: <<http://www.vmware.com>>. Acesso em: 18 jun. 2007.

- [11] MAIA, Garilan. **Máquinas Virtuais**: avaliação de desempenho e consolidação de servidores. Gravataí: ULBRA, 2005. Monografia, Faculdade de Ciência da Computação. Universidade Luterana do Brasil, 2005.
- [12] **SERVICE IT SOLUTIONS**. Disponível em <<http://www.service.com.br>>. Acesso em: 18 jun. 2007.
- [13] **VIRTUALIZATION.INFO. Security by Virtualization**. Disponível em: <<http://http://www.virtualization.info/2006/07/security-by-virtualization.html>>. Acesso em: 18 jun. 2007.
- [14] **NATIONAL INFORMATION ASSURANCE PARTNERSHIP. Common Criteria Evaluation and Validation Scheme Validation Report For VMware ESX Server 2.5.0 and VirtualCenter 1.2.0**. Disponível em: <[http://niap.bahialab.com/cc-scheme/st/ST\\_VID10056-VR.pdf](http://niap.bahialab.com/cc-scheme/st/ST_VID10056-VR.pdf)>. Acesso em: 03 mar. 2007.
- [15] **INFOGARD LABORATORIES INC. VMware ESX Server 2.5.0 and VMware VirtualCenter 1.2.0 Security Target**. Disponível em: <[http://niap.bahialab.com/cc-scheme/st/ST\\_VID10056-ST.pdf](http://niap.bahialab.com/cc-scheme/st/ST_VID10056-ST.pdf)>. Acesso em: 03 mar. 2007.
- [16] **CSE: Products in Evaluation**: Disponível em: <<http://www.cse-cst.gc.ca/services/common-criteria/ongoing-evals-e.html>>. Acesso em: 18 jun. 2007.
- [17] **REFLEX SECUTIRY. Virtual Security Appliance**. Disponível em: <[http://www.reflexsecurity.com/reflex\\_vsa.php](http://www.reflexsecurity.com/reflex_vsa.php)>. Acesso em: 18 jun. 2007.
- [18] **ABNT NBR ISO/IEC 17799:2005**. Tecnologia da Informação – Técnicas de Segurança – Código de Prática para a Gestão da Segurança da Informação. Rio de Janeiro: ABNT, 2005.
- [19] POPEK G.; GOLDBERG, R. **Formal Requirements for Virtualizable Third Generation Architectures. Communications of the ACM**. [S.l], v. 17, n. 7, p. 412-421, 1974.
- [20] **SERVICE IT SOLUTIONS. Pesquisa de Avaliação de Ambientes Virtuais**. Disponível em: <<http://www.service.com.br>>. Acesso em: 15 maio 2007.
- [21] VARIAN, Melinda. **VM and the VM Community: Past, Present, and Future**. Disponível em: <<http://www.princeton.edu/~melinda/25paper.pdf>>. Acesso em: 10 dez. 2006.

[22] LAUREANO, Marcos; MAZIERO, Carlos; JAMHOUR, Edgard. Proteção de Detectores de Intrusão através de Máquinas Virtuais. In: IV WSEG - WORKSHOP EM SEGURANÇA DE SISTEMAS COMPUTACIONAIS, 2004, Gramado. **Anais ...** Gramado: SBRC, 2004.

[23] WHITAKER, Andrew. *Building Robust Systems with Virtual Machine Monitors*. Disponível em: <<http://www.cs.washington.edu/homes/andrew/papers/general.pdf>>. Acesso em: 11 nov. 2006.

[24] VMware Inc. *Virtualization Overview*. Disponível em: <<http://www.vmware.com/vmtn>>. Acesso em: 19 jun. 2007.

[25] VMware Inc. *Virtualization: Architectural Considerations and Other Evaluation Criteria*. Disponível em: <<http://www.vmware.com/vmtn>>. Acesso em: 19 jun. 2007.

[26] VMware Inc. *ESX Server: Security White Paper*. Disponível em: <<http://www.vmware.com/vmtn>>. Acesso em: 19 jun. 2007.

[27] *XENSOURCE*. Disponível em: <<http://www.xensource.com/>>. Acesso em: 18 jun. 2007.

[28] *PLEX86 VIRTUAL MACHINE PROJECT*. Disponível em: <<http://plex86.sourceforge.net/>>. Acesso em: 18 jun 2007.

[29] Fundação CEEE. **FAQ Perguntas Frequentes Linux**. Porto Alegre: Fundação CEEE, 2007.