

UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
CURSO DE TECNOLOGIA EM SISTEMAS PARA INTERNET

RICARDO MOTTA DUCHESQUI

**AMBIENTE VIRTUALIZADO DE PEQUENO PORTE PARA
CONSOLIDAÇÃO DE SERVIDORES**

TRABALHO DE CONCLUSÃO DE CURSO

TOLEDO

2017

RICARDO MOTTA DUCHESQUI

**AMBIENTE VIRTUALIZADO DE PEQUENO PORTE PARA
CONSOLIDAÇÃO DE SERVIDORES**

Trabalho de Conclusão de Curso de Graduação, apresentado ao Curso Superior de Tecnologia em Sistemas para Internet, da Universidade Tecnológica Federal do Paraná – UTFPR, como requisito parcial para obtenção do título de Tecnólogo.

Orientador: Me. Alexandre Augusto Giron

TOLEDO

2017

Ricardo Motta Duchesqui

AMBIENTE VIRTUALIZADO DE PEQUENO PORTE PARA CONSOLIDAÇÃO DE SERVIDORES

Este Trabalho de Conclusão de Curso de Graduação foi julgado e aprovado como requisito parcial para a obtenção do Título de Tecnólogo em Sistemas para Internet, do curso de Tecnologia em Sistemas para a Internet da Universidade Tecnológica Federal do Paraná (UTFPR).

Toledo, 29 de novembro de 2017.

Prof. Fábio Engel de Camargo, Me.
Coordenador de Curso
Tecnologia em Sistemas para a Internet

Prof. Wilson Dalle Molle, Dr
Responsável pelos Trabalhos de Conclusão de Curso

ORIENTAÇÃO

Alexandre Augusto Giron, Me.
Universidade Tecnológica Federal do Paraná
Orientador

BANCA EXAMINADORA

Fábio Engel de Camargo, Me.
Universidade Tecnológica Federal do Paraná

André Luiz Barros Luchesi, B.Sc.
Universidade Tecnológica Federal do Paraná

“The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it.” (WEISER, 1991)

“As tecnologias mais profundas são aquelas que desaparecem. Elas se entrelaçam no tecido da vida cotidiana até se tornarem indistinguíveis.” (WEISER, 1991)

RESUMO

DUCHESQUI, Ricardo M. Ambiente Virtualizado de Pequeno Porte para Consolidação de Servidores. 2017. 89 p. Trabalho de conclusão de curso – Tecnologia em Sistemas para Internet, Universidade Tecnológica Federal do Paraná. Toledo, 2017.

Em um modelo tradicional de infraestrutura de TI tem-se vários servidores dedicados, cada um fornecendo um determinado serviço. Esse modelo de infraestrutura gera vários problemas para a empresa, pois com vários servidores físicos a administração é mais complexa, o espaço ocupado é maior, o consumo de energia é elevado entre outros problemas, além disso os recursos de hardware muitas vezes são subutilizados. Com a virtualização muitos desses problemas são solucionados, em um ambiente virtualizado é possível mudar rapidamente a infraestrutura fazendo uso de componentes lógicos que são independentes de hardware, além de permitir ajustar e distribuir os recursos de hardware entre as máquinas virtuais, favorecendo o compartilhamento desses recursos. A proposta deste trabalho é trazer a virtualização para o cenário da pequena empresa, pois na maioria das vezes só se ouve falar de virtualização em grandes empresas. Por meio da homologação de um conjunto de hardware de baixo custo e utilizando ferramentas gratuitas de virtualização, foi configurado um ambiente de pequeno porte para consolidação de servidores, na qual foram consolidados servidores com os serviços mais comuns utilizados em uma pequena empresa. Com o ambiente configurado, foram realizados testes de sobrecarga dos principais recursos de hardware como CPU, memória, acesso a disco e rede, e com isso obtidos dados para validar a implantação desse ambiente em um cenário real de uma pequena empresa. Os resultados dos testes mostram que, se os recursos de hardware forem levados a um estado de uso intenso, poderão comprometer o desempenho do ambiente todo. No entanto, as situações simuladas nos testes podem não acontecer em um cenário real, e se ocorrerem, até mesmo em ambientes de grande porte podem apresentar problemas. Portanto, a configuração, monitoramento e correta distribuição dos recursos de hardware no ambiente, ajudarão a evitar o comprometimento do desempenho do ambiente virtualizado.

Palavras-chave: Virtualização. Pequeno Porte. Consolidação de Servidores. Infraestrutura de TI. Infraestrutura de TI de Pequeno Porte.

ABSTRACT

DUCHESQUI, Ricardo M. Small Business Virtualized Environment for Server Consolidation. 2017. 89 p. End-of-Course Paper – Internet Systems Technology, Federal University of Technology-Paraná. Toledo, 2017.

In a traditional IT infrastructure model there are several dedicated servers, each one providing a certain service. This infrastructure model causes several problems for the company, because with several physical servers the administration is more complex, the space occupied is bigger, the energy consumption is high among other problems, in addition the hardware resources are often underutilized. With virtualization many of these problems are solved, in a virtualized environment it is possible to quickly change the infrastructure by making use of logical components that do not depend on hardware, as well as allowing to adjust and distribute the hardware resources between the virtual machines, favoring the sharing of these resources. The purpose of this paper is to bring virtualization to the small business scenario, since most of the time we only hear about virtualization in large companies. Through the approval of a set of low cost hardware and using free virtualization tools, a small server consolidation environment was configured, in which servers with the most common services used in a small company were consolidated. With the environment configured, overload tests of the main hardware resources such as CPU, memory, disk access and network were carried out, and with this data were obtained to validate the implementation of this environment in a real small company scenario. The test results show that if the hardware resources are brought to an intense use condition, they can compromise the performance of the entire environment. However, simulated test situations may not happen in a real world scenario, and if they occur, even in large business environments, problems may arise. Therefore, configuring, monitoring, and correctly distributing hardware resources in a given environment will help to avoid compromising the performance of the virtualized environment.

Keywords: Virtualization. Small Business. Consolidation of Servers. IT infrastructure. Small Business IT Infrastructure.

LISTA DE FIGURAS

Figura 1 - Organização dos componentes em uma Máquina Virtual.....	16
Figura 2 - Hypervisor tipo 1	18
Figura 3 - Hypervisor tipo 2	19
Figura 4 - Modos de operação na arquitetura de processadores x86	20
Figura 5 - Infraestrutura tradicional de TI (servidores dedicados)	24
Figura 6 - Infraestrutura de TI com ambiente virtualizado	25
Figura 7 – Quadrante mágico das soluções de virtualização para x86	27
Figura 8 – Gráfico de tempo de compilação de carga de trabalho SQL	32
Figura 9 – Configuração e execução da ferramenta <i>LoadStorm</i>	40
Figura 10 – Leitura de memória no SO convidado após a sobrecarga	44
Figura 11 – Configuração dos discos no RAID 10.....	45
Figura 12 – Informação de tempo de busca e latência de cada disco.....	45
Figura 13 – VMs ligadas em um mesmo vSwitch e uma interface física	50
Figura 14 – Organização da rede virtual e física no ambiente do ESXI	50
Figura 15 – Tráfego de rede em uma VM e na interface física do ESXI	52
Figura 16 – Tráfego de rede em duas VM e na interface física do ESXI.....	52

LISTA DE SIGLAS

TI	Tecnologia da Informação
SO	Sistema Operacional
OS	<i>Operating System</i>
TCO	<i>Total Cost Ownership</i>
VM	<i>Virtual Machine</i>
ERP	<i>Enterprise Resource Planning</i>
SGBD	Sistema Gerenciador de Banco de Dados
IBM	<i>International Business Machines</i>
CPU	<i>Central Processing Unit</i>
RAM	<i>Random Access Memory</i>
VMM	<i>Virtual Machine Monitor</i>
IO	<i>Input Output</i>
PDC	<i>Primary Domain Controller</i>
HCL	<i>Hardware Compatibility List</i>
SATA	<i>Serial Advanced Technology Attachment</i>
RAID	<i>Redundant Array of Independent Disks</i>
GbE	<i>Gigabit Ethernet</i>
BIOS	<i>Basic Input/Output System</i>
UI	<i>User Interface</i>
NFS	<i>Network File System</i>
NTP	<i>Network Time Protocol</i>
GPS	<i>Global Positioning System</i>
OVF	<i>Open Virtualization Format</i>
OVA	<i>Open Virtual Appliance</i>
SMS	<i>Short Message Service</i>

LISTA DE TABELAS

Tabela 1 – Resumo comparativo das versões gratuitas dos principais <i>hypervisors</i> ..	31
Tabela 2 – Percentual de memória livre nos ambientes virtualizados	33
Tabela 3 – Desempenho de rede nos ambientes virtualizados	33
Tabela 4 – Desempenho de CPU nos ambientes virtualizados.....	34
Tabela 5 – Hardware homologado para o projeto e preços em julho de 2017	36
Tabela 6 – Requisitos de hardware para cada serviço e hardware das VMs	37
Tabela 7 – Percentual de uso de CPU no ESXI e em cada VM antes do teste.....	39
Tabela 8 – Percentual de uso de CPU no ESXI e em cada VM durante o teste	40
Tabela 9 – Percentual de uso de CPU no ESXI e em cada VM durante os testes....	41
Tabela 10 – Informações de memória nos SOs convidados antes da sobrecarga....	43
Tabela 11 – Informações de memória nos SOs convidados durante a sobrecarga ..	44
Tabela 12 – IOPS para taxas de leituras e escritas diferentes em RAID 10	46
Tabela 13 – Testes executados com o <i>IO Analyzer</i>	47
Tabela 14 – Resultado dos testes de acesso a disco	48
Tabela 15 – Resumo dos testes de sobrecarga do ambiente virtualizado	53

SUMÁRIO

1	INTRODUÇÃO.....	11
2	OBJETIVOS	14
2.1	OBJETIVO GERAL	14
2.2	OBJETIVOS ESPECÍFICOS.....	14
3	VIRTUALIZAÇÃO.....	15
3.1	DEFINIÇÃO DE MÁQUINAS VIRTUAIS	16
3.2	EMULADORES E MÁQUINAS VIRTUAIS	17
3.3	CATEGORIAS DE VIRTUALIZAÇÃO	17
3.4	TIPOS DE HYPERVISOR.....	18
3.5	VIRTUALIZAÇÃO NA PLATAFORMA X86.....	19
3.6	VIRTUALIZAÇÃO TOTAL E PARAVIRTUALIZAÇÃO	20
3.7	VANTAGENS DA VIRTUALIZAÇÃO	21
4	METODOLOGIA.....	23
4.1	PRINCIPAIS HYPERVISORS DO MERCADO	25
4.1.1	VMWARE ESXI	27
4.1.2	MICROSOFT HYPER-V	29
4.1.3	CITRIX XENSERVER.....	30
4.1.4	RESUMO COMPARATIVO DOS PRINCIPAIS HYPERVISORS EM SUAS VERSÕES GRATUITAS.....	30
4.2	DESEMPENHO DE VMS NO ESXI, HYPER-V E XENSERVER.....	32
4.3	VMWARE ESXI HYPERVISOR ESCOLHIDO PARA O PROJETO.....	34
4.4	CONJUNTO DE <i>HARDWARE</i> HOMOLOGADO PARA O ESXI	35
4.5	CONFIGURAÇÃO DE <i>HARDWARE</i> VIRTUAL DAS VMS NO AMBIENTE	37
4.6	TESTES DE DESEMPENHO E RESULTADOS	38
4.6.1	SOBRECARGA DE CPU.....	39
4.6.2	SOBRECARGA DA MEMÓRIA	42
4.6.3	SOBRECARGA DO ACESSO A DISCO	45
4.6.4	SOBRECARGA DO TRÁFEGO DE REDE.....	49
4.6.5	COMPARATIVO DOS TESTES REALIZADOS E DISCUSSÕES	53
5	CONCLUSÃO.....	55

REFERÊNCIAS.....	56
APÊNDICE A – INSTALAÇÃO E CONFIGURAÇÃO DO VMWARE ESXI 6.5	60

1 INTRODUÇÃO

Para entrar no conceito de virtualização é necessário entender a definição de infraestrutura de Tecnologia da Informação (TI). A infraestrutura de TI pode ser considerada o alicerce do modelo operacional das empresas na qual seus negócios são baseados na informação, ou seja, é a parte que suporta as aplicações, e por sua vez sustentam os processos (VERAS, 2016).

Os modelos de negócios das empresas se caracterizam por uma intensa competição, surgimento de produtos substitutos, maior exigência dos clientes, concorrência global e ciclo de vida curto de produtos e serviços, isso faz com que os negócios sejam dinâmicos exigindo um alinhamento da infraestrutura de TI a esse dinamismo (FERNANDES e DE ABREU, 2014). Em um modelo tradicional de infraestrutura de TI tem-se vários servidores dedicados, cada um fornecendo um tipo de serviço. Para as empresas em que tanto os clientes como a própria organização se reconfigura a todo momento, esse modelo de infraestrutura não é eficaz.

Na situação em que a empresa necessite de mais algum serviço em seu ambiente, é necessário à aquisição de um novo *hardware* e a configuração e instalação do novo serviço. Por outro lado, caso ocorra algum problema em algum dos servidores que já estejam em operação também exigirá uma série de manobras para fazer com que o serviço seja reestabelecido. O desligamento ou reinicialização do servidor, a troca de algum componente de *hardware*, reinstalação do Sistema Operacional (SO) e serviços, seriam algumas das operações críticas.

No modelo tradicional de servidores dedicados é visível que não existe muito dinamismo nos processos que envolvem a infraestrutura de TI, além do não aproveitamento dos recursos de *hardware* em sua totalidade. Uma pesquisa conduzida por Seruya (2013) constatou que na maioria das vezes em um servidor x86 dedicado executando um único serviço a taxa de aproveitamento é de 10% a 20% dos recursos de hardware, sendo que os outros 80% a 90% ficam ociosos. Além disso existem outras questões a considerar, tais como:

- A administração e gerenciamento de múltiplos servidores dedicados é uma tarefa complexa.
- Com múltiplos equipamentos ligados o consumo de energia elétrica precisa ser considerado.

- Necessidade de manter um ambiente climatizado e grande espaço físico para acomodar todos os servidores.
- Para cada novo serviço, é necessário à aquisição de novo *hardware* aumentando o Custo Total de Propriedade (TCO) *Total Cost of Ownership* da empresa.
- O processo de instalação de cada novo serviço em um servidor dedicado demanda vários passos e configurações, consumindo tempo, para o profissional alocado na realização do serviço.
- A migração de um servidor para um novo *hardware* ou restauração em caso de desastre é uma tarefa demorada.
- Backups precisam ser gerenciados em cada servidor individualmente, além disso, **não é possível ter (*snapshots*) que guardam um estado congelado do sistema**. Diferente de pontos de restauração que estão no nível do SO convidado, o *snapshot* é gerenciado no nível das máquinas virtuais com maior velocidade e funcionalidade.

Para solucionar esses problemas as empresas buscam formas de construir infraestruturas de TI estáveis e escaláveis em cenários dinâmicos. Com a virtualização isso é possível, além de solucionar as questões citadas anteriormente. Em um ambiente virtualizado é possível mudar rapidamente a infraestrutura fazendo uso de componentes lógicos que são independentes de hardware (VERAS, 2016), além de permitir ajustar e distribuir o uso dos recursos de hardware entre as máquinas virtuais, favorecendo o compartilhamento desses recursos.

A virtualização desvincula as aplicações e o sistema operacional dos recursos físicos e acaba por agilizar e permitir o surgimento de uma plataforma virtual. Servidores virtuais são mais fáceis de serem instalados, gerenciados e migrados para o novo ambiente. Também os ambientes de teste e desenvolvimento, necessários para a manutenção de aplicações empresariais, são facilmente montados com a otimização dos recursos produzida pela virtualização. (VERAS, MANOEL. 2016, cap. 1).

Pequenas empresas geralmente utilizam um conjunto de serviços que são essenciais para um bom funcionamento dos negócios, como Sistema de Gestão Empresarial do tipo ERP (*Enterprise Resource Planning*) juntamente com um Sistema Gerenciador de Banco de Dados (SGBD), serviço de diretório e domínio para gerenciar seus usuários, servidor de arquivos, *firewall* e filtro de conteúdo web, servidor de aplicação web, além de outros serviços que dependerão do segmento da

empresa. Devido às características desses serviços fica clara a necessidade de utilização de servidores para mantê-los, e no modelo de servidores dedicados, na maioria das vezes cada um desses serviços fica em um servidor físico.

O objetivo desse trabalho é selecionar dentre os *softwares* de virtualização, os que possuem versões gratuitas, e que permitam criar um ambiente virtualizado de pequeno porte. Além disso, deve ser possível consolidar um conjunto de servidores virtualizados com os seguintes serviços: Servidor de Banco de Dados; Controlador de domínio e diretório juntamente com servidor de arquivos; *firewall* e filtro de conteúdo web; Servidor de aplicação web.

No capítulo 2 desse documento é abordado o objetivo geral e objetivos específicos do projeto. No capítulo 3 é feito o embasamento do trabalho com o referencial teórico sobre virtualização e de outras tecnologias, no capítulo 4 é apresentado a metodologia utilizada e tecnologias empregadas para atingir os objetivos específicos e como estes levam ao objetivo geral. E por fim, no capítulo 5 as conclusões e expectativas para trabalhos futuros.

2 OBJETIVOS

Nessa seção será apresentado o objetivo geral do projeto e objetivos específicos que permitirão a conclusão do trabalho.

2.1 OBJETIVO GERAL

Selecionar dentre os softwares de virtualização, um que possua versão gratuita, e viabilizar um ambiente virtualizado de pequeno porte para consolidação de servidores, na qual deve suportar os seguintes serviços: i) Servidor de banco de dados, ii) Controlador de domínio, diretório e servidor de arquivos, iii) *Firewall* e filtro de conteúdo web, iv) Servidor de aplicação web.

2.2 OBJETIVOS ESPECÍFICOS

- ✓ Discutir as tecnologias de virtualização e suas aplicações.
- ✓ Selecionar dentre as plataformas de virtualização (*hypervisor*) gratuitas uma que permita a configuração de um ambiente virtualizado de pequeno porte com foco em um conjunto de serviços distribuídos entre 3 a 4 VMs (Virtual Machine) ou máquinas virtuais.
- ✓ Homologar um conjunto de *hardware* compatível com o *software* de virtualização escolhido.
- ✓ Realizar a instalação e configuração dos servidores virtualizados no ambiente.
- ✓ Realizar testes de sobrecarga e monitoramento dos recursos de *hardware* compartilhados, e assim verificar o impacto causado no ambiente virtualizado e nos serviços em execução nas VMs.
- ✓ Produzir um manual de instalação e configuração do ambiente virtualizado.

3 VIRTUALIZAÇÃO

Segundo Laureano (2006), o termo virtualização tem origem na década de 1950, naquela época foi criado o conceito de memória virtual, utilizada nos sistemas operacionais modernos. A memória virtual desvincula os endereços físicos de memória daqueles vistos pelas aplicações, assim os programas podem ser alocados em qualquer região não contígua, permitindo o compartilhamento de forma segura, além de resolver o problema da limitação física da memória.

Em meados de 1960 os computadores eram conhecidos como *mainframe*, computador de grande poder computacional e de custo elevado, esses se tornaram indispensáveis para a solução de problemas daquela época.

Para conseguir compartilhar o uso desses equipamentos, na mesma época foi criado o conceito de *time-sharing* que permitia o uso de um mesmo equipamento por vários usuários de forma transparente, sem que um percebesse a presença de outro. Porém com compartilhamento de aplicações que podem conter falhas e vulnerabilidades em um mesmo equipamento, todo o sistema computacional ficava exposto, o que poderia comprometer o funcionamento do conjunto todo (MATTOS, 2009).

Outra proposta que surgiu foi de utilizar vários computadores em rede um para cada usuário, isso proveria o isolamento e melhor desempenho, porém era uma solução que aumentaria o custo e desperdício computacional.

Com isso a IBM começou a trabalhar na primeira máquina virtual para sua linha *mainframes* 370, eles desenvolveram o sistema CP67, nele uma camada de virtualização de *hardware* permitia compartilhar os recursos em unidades lógicas autônomas, assim era possível desvincular o SO do *hardware* real, permitindo instâncias até do mesmo sistema operacional (LAUREANO, 2006).

Nos anos de 1970 e 1980 ocorreu o barateamento do *hardware* e o aumento da comercialização de computadores pessoais, fazendo com que o uso das máquinas virtuais fosse deixado de lado. Já em 1990 aparentemente a virtualização estava condenada, mas alguns anos depois surgiram novas tecnologias de virtualização, capazes de serem instaladas nas plataformas x86. (SERUYA, 2014).

3.1 DEFINIÇÃO DE MÁQUINAS VIRTUAIS

Para Marshal et al. (2006) máquina virtual é um ambiente de execução único e isolado que é criado por meio de uma camada de *software* de virtualização, que parece ser quase exatamente como um computador físico.

Veras (2016) define uma máquina virtual como um *container* de *software*, que prove isolamento entre as outras VMs, e com capacidade de executar sistemas operacionais e aplicações como se fosse uma máquina física. Ela possui todos os recursos de uma máquina real, CPU, memória RAM, disco rígido e interface de rede virtuais baseadas em *software*. As diferenças entre uma máquina virtual e uma física, não são notadas por um SO, aplicativo ou outros computadores em rede. A Figura 1 mostra a organização dos componentes de uma máquina virtual.

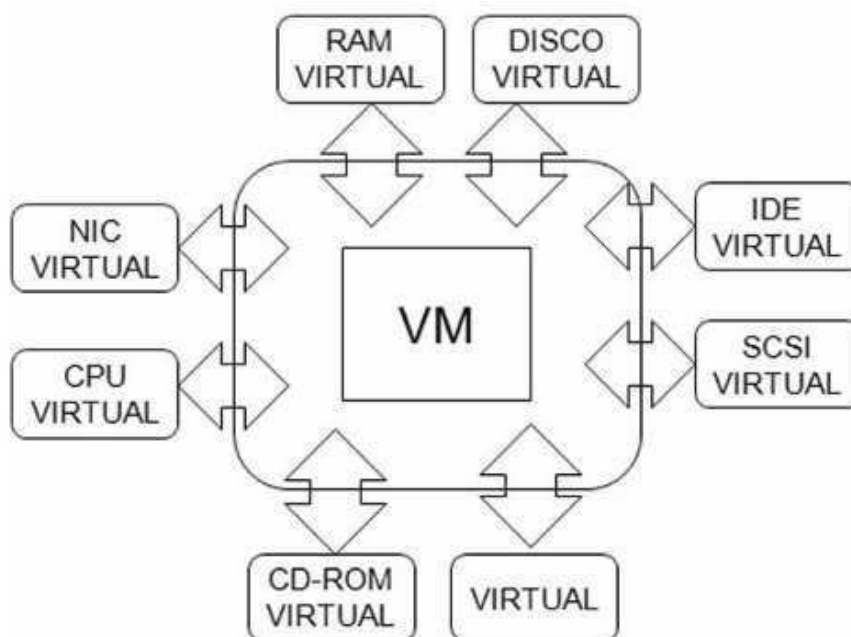


Figura 1 - Organização dos componentes em uma Máquina Virtual
Fonte: Veras (2016)

3.2 EMULADORES E MÁQUINAS VIRTUAIS

Em um emulador as instruções realizadas por uma máquina real são implementadas em uma camada de *software* abstrata, possibilitando a execução de um aplicativo de uma plataforma em outra, por exemplo, um aplicativo desenvolvido para i386 executando em uma plataforma *Sparc*, o emulador simula um computador real, ou seja, transcreve as instruções de um processador alvo para o processador em execução (LAUREANO, 2006).

Nota-se que na emulação pode ocorrer a perda de eficiência, pois todas as instruções da máquina real precisam ser traduzidas, além disso, são complexos por terem de simular quase todas as instruções do processador.

A máquina virtual está numa posição intermediária entre o emulador e a máquina real, assim os recursos de *hardware* são abstraídos para o sistema operacional e aplicativos. Essa abstração é criada por um monitor de máquina virtual VMM (*Virtual Machine Monitor*). O monitor de máquinas virtuais também é conhecido como *hypervisor*, ele cria e gerencia todas as máquinas virtuais, e fornece uma interface de multiplexação de *hardware* que é idêntica ao *hardware* subjacente (LAUREANO, 2006).

3.3 CATEGORIAS DE VIRTUALIZAÇÃO

Para Carissimi (2008) a virtualização ocorre em uma camada de software que transforma as ações de um determinado sistema A para outro sistema B equivalente, assim é possível classificar os softwares de virtualização em três categorias:

Nível de hardware: nessa categoria a camada de virtualização fica diretamente no hardware e apresenta uma abstração do hardware real para as camadas superiores. Essa era a definição das primeiras máquinas virtuais criadas pela IBM.

Nível de software: um mecanismo cria partições lógicas em uma plataforma e essa partição é considerada uma máquina isolada, mas que compartilha o mesmo

SO. Nesse modelo a camada de virtualização fica entre o sistema operacional e as aplicações.

Nível de linguagem de programação: a camada virtualizada é uma aplicação do sistema operacional. Assim uma máquina abstrata executa uma aplicação desenvolvida em uma linguagem de alto nível.

3.4 TIPOS DE HYPERVISOR

O *hypervisor* ou VMM é a camada de *software* de virtualização responsável por controlar os acessos requisitados pelas máquinas virtuais, fazer o gerenciamento de memória e manutenção do estado dessas máquinas. O desempenho e escalabilidade da virtualização estão associados ao tipo de *hypervisor* utilizado, a agilidade na configuração dos recursos computacionais sem interromper a VM e segurança sobre os recursos compartilhados são alguns dos pontos para se considerar em um bom *hypervisor* (VERAS, 2016).

Ainda segundo Veras (2016) de uma forma simplificada consideram-se dois tipos de *hypervisor*:

Tipo 1: esse tipo apresenta um ótimo desempenho, pois é instalado diretamente no *hardware* físico e as máquinas virtuais são colocadas sobre ele. Sua função é compartilhar os recursos físicos (processador, memória, meios de armazenamento e dispositivos de I/O) entre as diferentes máquinas virtuais (Figura 2).



Figura 2 - Hypervisor tipo 1
Fonte: Adaptado de Laureano (2006)

Tipo 2: é executado como um processo sobre um sistema operacional hospedeiro. A camada de virtualização é composta por um sistema operacional convidado e por um *hardware* virtual criado sobre os recursos de *hardware* oferecidos através do SO nativo, conforme mostra a Figura 3.



Figura 3 - Hypervisor tipo 2
Fonte: Adaptado de Laureano (2006)

3.5 VIRTUALIZAÇÃO NA PLATAFORMA X86

A implementação da virtualização na arquitetura x86 não é uma tarefa simples, pois os processadores desenvolvidos para essa arquitetura não previam dar suporte para virtualização, além disso, os sistemas operacionais assumem que tem o controle total do *hardware*.

A arquitetura x86 trabalha com quatro modos de operação de processador, identificada de 0 a 3, chamados de anéis de proteção (*rings*) visualizado na Figura 4. Nos sistemas Windows e Unix para essa plataforma apenas dois modos são usados: *ring 0* usado pelo sistema operacional e tem acesso privilegiado, e *ring 3* utilizado pelo modo usuário com menor privilégio. Quando um processo no modo usuário faz uma chamada para uma instrução privilegiada ocorre uma exceção (*trap*) que deve ser devidamente tratada pelo SO. A arquitetura x86 possui 17 instruções sensíveis, nos termos de arquitetura não são consideradas privilegiadas, mas na prática fazem acesso direto ao processador e podem causar *trap*, esse foi um grande desafio da

virtualização nessa plataforma. Nos anos 90 a VMWare, uma empresa do setor de virtualização, desenvolveu a técnica de translação binária para resolver esse problema, possibilitando que o *hypervisor* rodasse no *ring 0* e que o SO ficasse no *ring 3* em modo usuário, mas com menos privilégio que o *hypervisor* (VERAS, 2016).

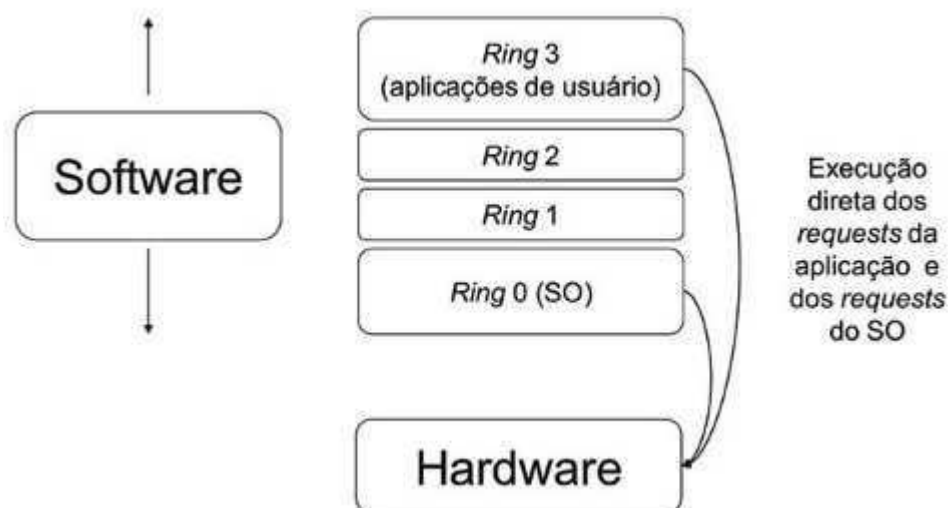


Figura 4 - Modos de operação na arquitetura de processadores x86
 Fonte: Veras (2016)

3.6 VIRTUALIZAÇÃO TOTAL E PARAVIRTUALIZAÇÃO

Na arquitetura x86 dependendo da forma como as instruções sensíveis são tratadas, a virtualização ou implementação do *hypervisor* pode ser obtida por meio de duas técnicas: virtualização total ou paravirtualização.

A virtualização total fornece uma abstração total do *hardware* adjacente, com isso o SO e aplicações executam como se estivessem na máquina real. A vantagem dessa técnica é que o SO convidado não precisa sofrer modificações para ser virtualizado. No entanto o *hypervisor* precisa prover um conjunto de *hardware* genérico, que pode acarretar na subutilização do *hardware* real, e todas as instruções precisam ser testadas no *hypervisor* para verificar se são instruções sensíveis (CARISSIMI, 2008).

A paravirtualização é considerada uma alternativa aos problemas encontrados na virtualização total. Nessa técnica o SO convidado é modificado e

sempre que uma instrução sensível for executada fará a chamada direto para o *hypervisor*, além disso, os acessos ao *hardware* real são feitos por meio de drivers do próprio *hypervisor*, que garante uma melhora no desempenho (CARISSIMI, 2008).

Com o passar dos anos os fabricantes de processadores investiram em extensões na arquitetura para suportar virtualização assistida por *hardware* e melhorar o desempenho, praticamente eliminando as diferenças existentes entre as duas técnicas citadas. Tanto a Intel (Intel VT) e AMD (AMD-V) trabalharam para modificar os modos de operação dos processadores, os anéis (*rings*) de proteção, com isso o *hypervisor* passou a trabalhar em um anel abaixo do *ring 0* criado especificamente para melhorar o desempenho de servidores da plataforma x86 (VERAS, 2016).

3.7 VANTAGENS DA VIRTUALIZAÇÃO

De acordo com Pollon (2008) é possível destacar algumas das vantagens obtidas em um ambiente virtualizado:

Gerenciamento centralizado de servidores: com a redução do número de equipamentos físicos já garante a facilidade no gerenciamento dos equipamentos, assim como as ferramentas de gerenciamento fornecidas pelas plataformas de virtualização oferecem muitos recursos avançados de gerenciamento como: alocação de recursos para as máquinas virtuais em tempo de execução, migração de servidores físicos para o ambiente virtual, migração de servidores entre *hosts* sem o desligamento da VM, entre outros recursos.

Hospedagem eficiente de sistemas legados: sistemas legados tornam-se um problema para os administradores de rede, pois estão em sistemas operacionais que não oferecem mais suporte de atualização. O sistema legado não pode ser migrado para um SO mais recente ou *hardware* mais atual. Com a virtualização é possível instalar o SO defasado em uma VM e colocá-lo em um *hardware* mais atualizado e não subutilizar os recursos desse *hardware*.

Rápida disponibilização de ambiente de teste e treinamento: quando é necessário disponibilizar certo número de sistemas operacionais em um ambiente de

treinamento, essa tarefa se torna trivial no ambiente virtualizado, além de permitir fazer testes em sistemas antes de irem para a produção.

Disponibilização de ambiente de homologação de aplicativos e desenvolvimento: Com o isolamento fornecido pelas máquinas virtuais é possível testar novos aplicativos sem que isso interfira na operação de outros sistemas em execução.

Agilidade na recuperação de desastres: A recuperação de desastres geralmente leva um tempo considerável. Com a virtualização o processo de recuperação se torna mais ágil. Com a exportação da máquina virtual para um arquivo uma cópia na íntegra da VM é realizada, assim a tarefa de restauração é simples como realizar a cópia de arquivos, além disso, é possível salvar *snapshots* que são estados da máquina virtual que permitem voltar para esse estado caso alguma falha ocorra na VM.

Redução do custo de *hardware* e espaço físico: Com menos servidores em operação, conseqüentemente terá menos gastos com suporte e manutenção de *hardware* dos equipamentos, além de diminuir o espaço ocupado por eles.

Redução no consumo de energia: Com o aproveitamento total dos recursos de *hardware* por meio da virtualização, menos equipamentos serão necessários para manter os serviços. Por outro lado, existem os casos de sobrecarga em um único equipamento, o que causaria um maior consumo de energia, mas com a virtualização é possível delimitar o uso desses recursos evitando a sobrecarga.

4 METODOLOGIA

Como o objetivo do ambiente virtualizado é atender pequenas empresas e reduzir o (TCO) *Total Cost of Ownership*, a escolha de todos os componentes para a implantação do ambiente deve seguir critérios alinhados a esse cenário.

A escolha de uma plataforma de virtualização será feita dentre as existentes no mercado que atenda aos requisitos do projeto. Para essa seleção será considerado os seguintes critérios:

- ✓ Possuir versão de licenciamento gratuito que não tenha tempo de expiração, com objetivo de reduzir custo.
- ✓ Devem estar habilitados para um processador físico e no mínimo quatro núcleos, pois para melhor desempenho do ambiente algumas VMs poderão trabalhar com apenas um núcleo alocado para elas e outras com todos os núcleos, além de suportar pelo menos quatro núcleos por VM.
- ✓ O tipo de *hypervisor* deverá ser do tipo 1, considerando a proximidade que a camada de virtualização estará do *hardware* físico, para a melhora do desempenho do ambiente virtualizado.
- ✓ Possuir uma comunidade ativa na internet em vários fóruns ou sites, e com discussões sobre versões atuais das ferramentas. Sendo assim uma simples busca retornará uma grande quantidade de resultados com informações atuais e com a maior parte dos tópicos marcados como resolvidos.
- ✓ A empresa ou grupo responsável pelo *software* de virtualização deve ter produtos consolidados no mercado de virtualização, ou seja, deve ter sua plataforma de virtualização sendo utilizada em várias empresas, além de terem cases de sucesso que demonstrem as vantagens obtidas ao migrarem para a plataforma de virtualização.
- ✓ As VMs consolidadas no ambiente devem apresentar bom desempenho de IOPS (*Input/Output Operations Per Second*) nos discos e também no processamento, esses dados podem ser levantados por meio documentos fornecidos pela própria empresa ou artigos científicos que mostrem esses resultados.

- ✓ Possuir uma ferramenta de administração do ambiente virtualizado que seja de fácil utilização, e permita realizar a maior parte das operações nas VMs sem fazer uso da linha de comando, além de apresentar gráficos de uso de recursos do ambiente e registro de eventos.

Com a plataforma de virtualização selecionada, será necessária a homologação de um conjunto de *hardware*. A premissa aqui é a compatibilidade com a plataforma, tendo em vista que nem todo *hardware* funcionará com os *softwares* de virtualização.

O ambiente virtualizado de pequeno porte como em ambientes de grande porte, tem como objetivo mudar a infraestrutura tradicional de servidores físicos dedicados como pode ser visto na Figura 5, consolidando-os em um único *hardware* físico, e cada serviço sendo executado em uma VM mostrado na Figura 6.



Figura 5 - Infraestrutura tradicional de TI (servidores dedicados)
Fonte: Adaptação de VMware Visio stencils



Figura 6 - Infraestrutura de TI com ambiente virtualizado
Fonte: Adaptação de VMware Visio stencils

O ambiente virtualizado deverá se manter estável com todos os serviços sendo executados sem interferência de um sobre os outros. Para isso será feito uso de ferramentas que simulam o funcionamento dos serviços em uma situação de grande *stress*. Levando em consideração que acesso a disco, carga de processamento, uso de memória e tráfego de rede são fatores que podem impactar no desempenho do ambiente, esses recursos de *hardware* que serão testados.

4.1 PRINCIPAIS HYPERVISORS DO MERCADO

A evolução da tecnologia dos processadores e o suporte a virtualização assistida por *hardware*, fez com que surgisse inúmeras soluções de virtualização, tanto do tipo 1 como do tipo 2. VMware ESXI, Microsoft Hyper-V, Citrix XenServer, Oracle VM, Proxmox VE, KVM, XEN Project, Virtuozzo, LXC, Nutanix Acropolis, OpenVZ, Red Hat Virtualization etc., são alguns exemplos dessas ferramentas.

É notável a quantidade de opções disponíveis para realizar a implantação de um ambiente virtualizado, algumas dessas ferramentas são *opensource*, outras são

pagas, mas possuem uma versão gratuita com algumas limitações dos recursos disponíveis.

A Figura 7 apresenta o quadrante mágico das empresas de virtualização, mensurando um grau de competitividade entre as empresas (Gartner, 2016). O quadrante mágico é dividido em *leaders*, *visionaries*, *niche players* e *challengers* descritos a seguir:

- **Leaders:** possuem uma estratégia clara de seus produtos e compreendem bem o papel da virtualização, além disso possuem boas perspectivas para o futuro.
- **Visionaries:** tem uma abordagem ou produto diferenciado, compreendem bem o mercado de virtualização, mas não cumprem o seu potencial do ponto de vista de execução.
- **Niche players:** A virtualização é o mercado bem amplo, as empresas que estão nesse quadrante ou não possuem visão para sobressaírem ou estão focadas em segmentos específicos.
- **Challengers:** possuem uma forte habilidade para executar, mas têm uma visão de marketing ou produto focada.

O deslocamento no eixo horizontal (*completeness of vision*) no quadrante indica que, quanto mais a empresa avança nessa direção, mais integrada é sua visão atual e futura do mercado, ou seja, a empresa está aberta para integrar suas soluções com tecnologias emergentes, e também permitir a interoperabilidade com fornecedores externos.

Seguindo na vertical (*ability to execute*) diz respeito a qualidade e eficácia dos processos, sistemas, métodos e procedimentos que permitem que o desempenho do provedor de TI seja competitivo, eficiente e efetivo e afete positivamente a receita, retenção e reputação.

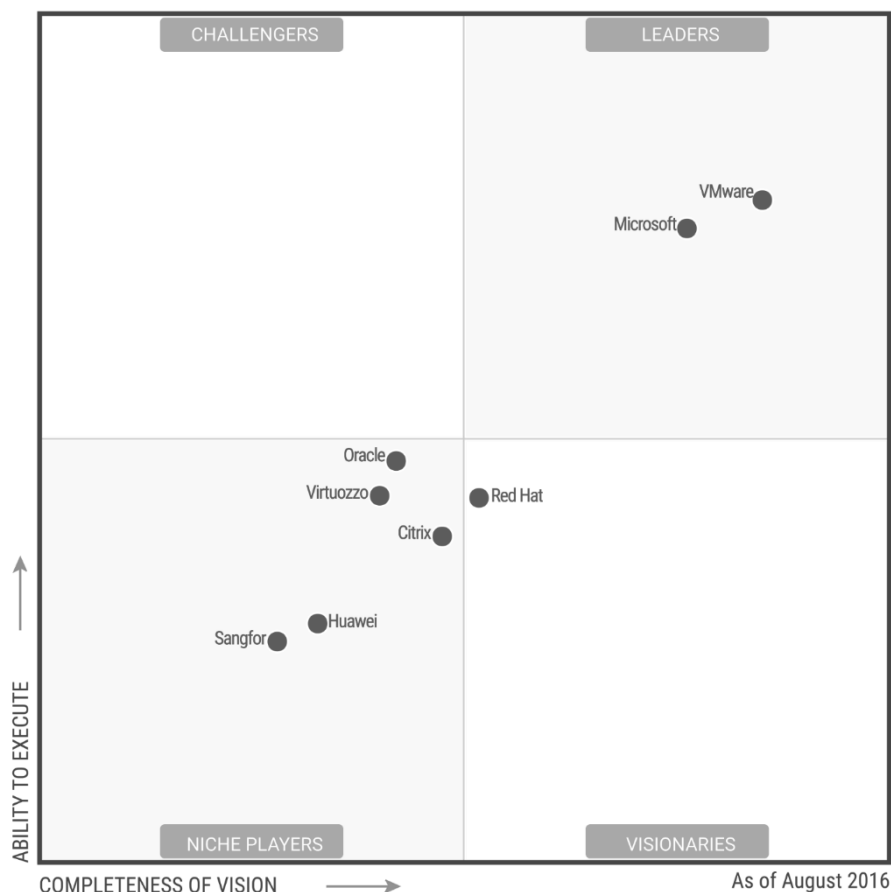


Figura 7 – Quadrante mágico das soluções de virtualização para x86
Fonte: Gartner

Seguindo os critérios já citados para a escolha de uma ferramenta de virtualização, foram selecionadas as três principais líderes do mercado: VMware ESXI, Microsoft Hyper-V e Citrix XenServer. A partir dessas escolhas foi feita a análise dos recursos fornecidos em suas versões gratuitas. Além disso foram utilizados os trabalhos de Manik e Arora (2016) e POLAST et al. (2016) que realizaram testes de desempenho em cada um dos ambientes, a partir desses dados foi feita a escolha de uma dentre as três para a implantação do ambiente de pequeno porte.

4.1.1 VMWARE ESXI

A VMWARE foi fundada em 1998 e sua meta era trazer a virtualização para a plataforma x86 e para indústria da computação pessoal. Mesmo as CPUs da

época não dando suporte a virtualização a VMWARE conseguiu fazer isso utilizando a técnica de tradução binária (TANENBAUM e BOS, 2016). Atualmente uma das principais soluções da VMWARE é o ESXI 6.5 um *hypervisor* do tipo 1 que possui uma arquitetura ultrafina que não depende de um sistema operacional hospedeiro e seu foco é a consolidação de servidores.

Os recursos do ESXI são disponibilizados por meio de licenças. De acordo com o tipo de licença escolhido, *Standard*, *Enterprise* e *Enterprise Plus* o ambiente virtualizado poderá contar com recursos como alta disponibilidade, proteção de dados, movimentação de VMs ligadas entre outros (VMWARE, 2017).

Para incentivar o uso de sua ferramenta a VMWARE disponibiliza uma versão gratuita, que de acordo com VMWARE (2017) conta com suporte para os seguintes recursos:

- ✓ 2 CPUs físicas (sockets).
- ✓ Core ilimitados por CPU.
- ✓ Memória RAM ilimitada, limitada somente pelo *hardware*.
- ✓ 8 vCPU por VM.
- ✓ Memória RAM por VM limitada pela arquitetura e quantidade física.
- ✓ A licença gratuita nunca expira.
- ✓ A administração do ambiente pode ser feita por uma interface WEB desenvolvida em HTML 5 ou por meio de um *software desktop* para o Sistema Operacional Windows.
- ✓ Faz uso do sistema de arquivos VMFS (Virtual Machine File System) otimizado para armazenar imagens de disco das VMs.
- ✓ Possui uma ferramenta para P2V (Physical to Virtual) permite a conversão do SO de uma máquina física para uma VM.
- ✓ Pode ser instalado em um *Hard disk SD Card* ou *Pendrive*.
- ✓ ESXI suporta VMs com SOs de várias famílias: 18 versões de Windows, 54 versões de Linux, MACOS, Solaris, FreeBSD, etc.

A versão gratuita não dispõe de suporte do fabricante, agrupamento de hosts para formar um datacenter e movimentação de VMs ligadas entre hosts. No entanto para um ambiente na qual se deseja consolidar servidores com alguns

serviços para fazer o gerenciamento centralizado e o aproveitamento dos recursos de hardware o licenciamento gratuito será suficiente (VMWARE, 2017).

4.1.2 MICROSOFT HYPER-V

A Microsoft sempre acompanhou a evolução da virtualização, desde 2005 ela já possuía uma solução chamada *Virtual Server 2005*, voltada para a virtualização de servidores. Essa ferramenta evoluiu e em 2008 foi lançada com o nome de HYPER-V como parte integrante do *Windows Server*, mas também possui uma versão na qual não é necessário ter o *Windows Server* instalado para utilizar a ferramenta (OLIVEIRA, 2017).

A versão atual sem integração com *Windows Server* é conhecida como HYPER-V Server 2016. Segundo Microsoft (2016) sua distribuição é de forma totalmente gratuita com suporte para os seguintes recursos:

- ✓ 512 processadores lógicos.
- ✓ 24TB de memória RAM.
- ✓ 240 vCPU por VM.
- ✓ Memória RAM por VM até 16TB.
- ✓ Licença gratuita.
- ✓ Ferramenta de administração disponibilizado como um recurso do *Windows Server* integrada com o *Active Directory*, para utilizar fora do *Windows Server* é necessário fazer algumas configurações avançadas.
- ✓ Hyper-V suporta VMs com todas as versões de *Windows*, já Linux existe uma lista bem restrita.

4.1.3 CITRIX XENSERVER

O XENSERVER é um *hypervisor* do tipo 1, ele é mantido pela Citrix que a partir de 2013 liberou o seu código como um projeto *opensource* e com licenciamento GPL, isso significa que não é preciso pagar nada para utilizá-lo. Porém, caso seja necessário suporte é preciso adquirir uma versão *Enterprise* na qual possui suporte oferecido pela Citrix (CABRAL, 2015).

De acordo com Citrix (2017) a versão atual conhecida como XENSERVER 7.2 suporta os seguintes recursos:

- ✓ 288 processadores lógicos
- ✓ 5TB de memória RAM
- ✓ 32 vCPU por VM
- ✓ Memória RAM por VM até 1.5TB
- ✓ Licenciamento *OpenSource* GPL
- ✓ Possui uma ferramenta para *Windows* na qual permite o monitoramento e gerenciamento das VMs.
- ✓ Suporta VMs várias versões de *Windows* e Linux, algumas versões mais antigas de alguns SOs não são suportadas.

4.1.4 RESUMO COMPARATIVO DOS PRINCIPAIS HYPERVISORS EM SUAS VERSÕES GRATUITAS

A Tabela 1 mostra de forma resumida um comparativo dos principais *hypervisors* do mercado em suas versões gratuitas.

Tabela 1 - Resumo comparativo das versões gratuitas dos principais *hypervisors*

	ESXI 6.5	HYPER-V 2016	XENSERVER 7.2
CPU FÍSICO por HOST	2 CPUs físicas (sockets)	Até o total de núcleos suportados	Até o total de núcleos suportados
NÚCLEOS por HOST	Ilimitados por CPU	512	288
MEMÓRIA por HOST	Ilimitada	24 TB	5 TB
vCPU por VM	8 vCPU	240 vCPU	32 vCPU
MEMÓRIA por VM	Limitada pela arquitetura e quantidade física.	16 TB	1.5 TB
LICENÇA	Gratuita, nunca expira	Gratuita	Opensource GPL
ADMINISTRAÇÃO	WEB UI HTML 5, Versão Desktop Windows	Windows Server, Snap-in no Windows	Versão Desktop Windows
SISTEMA DE ARQUIVOS	VMFS (Virtual Machine File System)	NTFS e ReFS (Resilient File System)	EXT3
LOCAL DE INSTALAÇÃO	HARD DISK, SD Card ou Pendrive	HARD DISK	HARD DISK
SOs CONVIDADOS	18 versões de Windows, 54 versões de Linux, MACOS, Solaris, FreeBSD, etc.	Todas versões Windows, Linux lista restrita	Várias versões, SOs antigos não são suportados

Fonte: Site Microsoft, VMWare e CITRIX

4.2 DESEMPENHO DE VMS NO ESXI, HYPER-V E XENSERVEN

Segundo Veras (2016) existem dois conceitos fundamentais para considerar e que podem impactar um ambiente virtualizado: *workload* (carga de trabalho) e *throughput* (taxa de transferência).

Workload é composto dos dados a serem processados e as instruções que serão executadas sobre esses dados. Ele representa o desempenho do serviço que o usuário perceberá. O *workload* depende da aplicação processada, então ela varia no tempo, as vezes pode ser previsível e as vezes não, e impactará no desempenho da aplicação.

Throughput é definido como a capacidade do *hardware/software* em processar dados, é composto pela velocidade de I/O, velocidade de CPU, capacidade de paralelismo e eficiência do SO.

Em um trabalho de pesquisa realizado por Manik e Arora (2016), os autores criaram VMs com *Windows Server 2008 R2*, com configuração: 1 vCPU e 2GB de memória nos ambientes de virtualização ESXI, HYPER-V e XENSERVEN. Então eles executaram a compilação de uma consulta SQL com objetivo de medir o tempo gasto para a execução em cada ambiente. Nos testes foram considerados o tempo, processamento, memória e operações de leitura e escrita em disco, o resultado pode ser visto no gráfico da (Figura 8).

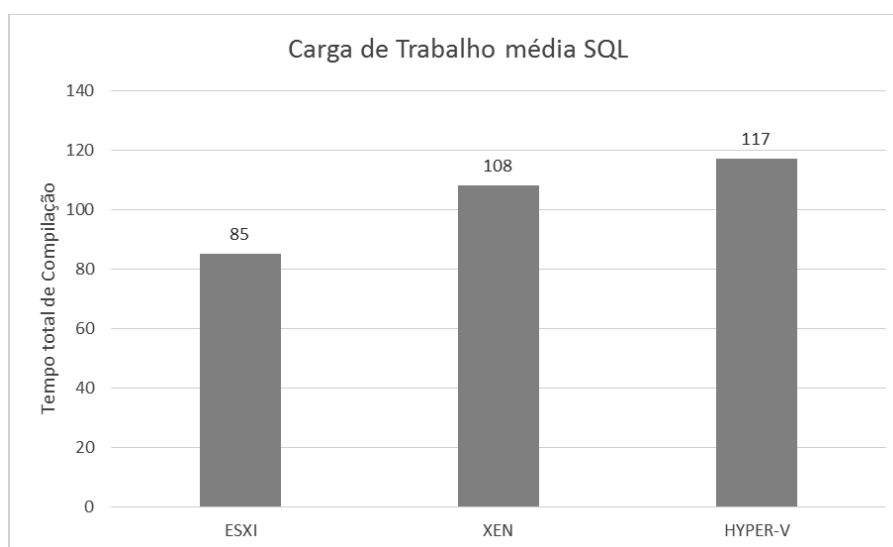


Figura 8 – Gráfico de tempo de compilação de carga de trabalho SQL
Fonte: Adaptado de (Manik e Arora, 2016)

Os resultados do gráfico da Figura 8 mostram como uma aplicação pode variar seu desempenho em cada ambiente. O gráfico mostra que o VMWare Esxi tem um desempenho ligeiramente melhor que os outros hypervisors.

Em outro trabalho conduzido por Polast et al. (2016), foram realizados testes de sobrecarga de recursos como memória, CPU e tráfego de rede nos ambientes virtualizados do ESXI, HYPER-V e XENSERVER. Para os testes foi utilizada uma VM configurada com o Microsoft Windows 2012 em cada ambiente, a ferramenta utilizada para simular as sobrecargas foi a Passmark.

Os resultados dos testes são mostrados a seguir, a Tabela 2 mostra o uso de memória, a Tabela 3 mostra o desempenho de rede e a Tabela 4 o desempenho de CPU em cada um dos ambientes. A métrica de CPU que a ferramenta fornece é uma métrica própria e quanto maior for o seu valor melhor é o desempenho da CPU.

Tabela 2 - Percentual de memória livre nos ambientes virtualizados

HYPERVERISOR	Memória disponível
ESXI	72,00%
HYPER-V	69,45%
XENSERVER	63,12%

Fonte: Adaptado de Polast et al. (2016)

Tabela 3 - Desempenho de rede nos ambientes virtualizados

HYPERVERISOR	Velocidade de envio em Mbps	Velocidade de recebimento em Mbps
ESXI	945	942
XENSERVER	930	925
HYPER-V	936	730

Fonte: Adaptado de Polast et al. (2016)

Tabela 4 - Desempenho de CPU nos ambientes virtualizados

HYPERVISOR	CPU Mark	Integer Mark	Op. Ponto Flutuante	Compressão	Ordenação	Single Threaded
ESXI	7750	14070	7365	11650	6960	1425
XENSERVER	7325	6870	6850	11630	6934	1285
HYPER-V	7716	14020	7358	11645	6954	1134

Fonte: Adaptado de Polast et al. (2016)

Os resultados dos testes realizados pelos autores, mostram que o ambiente virtualizado do ESXI apresentou melhor desempenho em todos os recursos sobrecarregados comparados com os outros ambientes virtualizados.

4.3 VMWARE ESXI HYPERVISOR ESCOLHIDO PARA O PROJETO

Com a análise das três principais ferramentas de virtualização do mercado, e considerando as suas versões gratuitas e recursos fornecidos nessas versões, pode-se concluir que qualquer uma delas conseguirá atender um ambiente de pequeno porte. Mas para este projeto será utilizado o ESXI da WMWARE. A justificativa da escolha do ESXI é dada pelos seguintes pontos:

- ✓ A VMWARE foi a primeira empresa a apresentar soluções de virtualização para a plataforma x86, isso a levou a solucionar muitos problemas como também a implementar otimizações.
- ✓ De acordo com o quadrante mágico do (GARTNER, 2016) a VMWARE é a empresa líder de mercado no fornecimento de soluções para virtualização.
- ✓ Possui compatibilidade com *hardware* fornecido por diversos fabricantes, isso facilita a utilização de um conjunto de *hardware* mais genérico para o *host* de virtualização.
- ✓ Possui ferramentas de fácil utilização para administração do ambiente virtualizado.

- ✓ Suporta inúmeras versões de SOs convidados, tanto versões atuais quanto mais antigas.
- ✓ Apresentou melhor desempenho sobre outras ferramentas de virtualização nos experimentos comparativo realizados por (MANIK e ARORA, 2016) e (POLAST et al., 2016).
- ✓ Familiaridade do pesquisador deste projeto com as ferramentas fornecidas pela VMWARE.

A instalação do ESXI, configurações necessárias para o ambiente virtualizado e a organização da rede e das VMs estão descritos no APÊNDICE A.

4.4 CONJUNTO DE *HARDWARE* HOMOLOGADO PARA O ESXI

A VMWARE recomenda a instalação do ESXI em um conjunto de *hardware* que esteja em sua lista de compatibilidade, *Hardware Compatibility List* (HCL), mas também não proíbe a utilização de *hardware* que estão fora de sua HCL. Muitos desses *hardwares* como *chipsets*, interfaces de rede, controladoras SATA, controladoras RAID entre outros, possuem compatibilidade com o ESXI a diferença é que não foram testados nos laboratórios da VMWARE, mas sim pelos fabricantes do *hardware* ou por usuários da ferramenta.

Outra exigência para a instalação do ESXI são os requerimentos mínimos que devem ser seguidos, caso contrário a instalação não avança ou poderá apresentar desempenho inferior ao esperado, o site da VMWARE destaca os seguintes requerimentos para a versão 6.5 do ESXI:

CPU

- ✓ Mínimo técnico: soquete único com dois núcleos.
- ✓ Mínimo recomendado: soquete duplo com quatro ou mais núcleos por CPU.

MEMÓRIA

- ✓ Mínimo técnico: 4 GB.
- ✓ Mínimo recomendado: 8 GB ou mais.

REDE

- ✓ Mínimo técnico: um único adaptador de rede de 1 GbE.
- ✓ Mínimo recomendado: dois adaptadores de rede de 1 GbE.

ARMAZENAMENTO

- ✓ Mínimo técnico: uma única unidade de 4 GB.
- ✓ Mínimo recomendado: unidades redundantes.

Para esse trabalho foram realizadas pesquisas na lista de compatibilidade da VMWARE, site das fabricantes de placas mães ASUS e ASRock, site da fabricante de dispositivos de rede TP-LINK, site da fabricante de controladoras raid ADAPTEC, assim como o fórum da comunidade VMWare, para encontrar um conjunto de *hardware* compatível. Com base nos dados levantados foi selecionado o conjunto de *hardware* mostrado na Tabela 5, na mesma tabela estão também os preços de cada peça e o custo total em julho de 2017:

Tabela 5 – Hardware homologado para o projeto e preços em julho de 2017

Qtd	Hardware	Preço R\$
1	Processador Intel Core i5 3.2GHz 6500 6ª Geração (4 Cores) com VT-x	749,99
1	Placa Mãe AsRock Pro4s h170 Socket 1151/SOM/REDE/VIDEO	409,90
1	Memória Kingston Hyper-X 16GB DDR4 2133MHz (1+1 8GB)	608,00
1	HD SSD Now Kingston A400 120GB 2.5" 3.0 6Gb/S	309,00
4	HDs SAMSUNG 1TB Sata 2 - F1-HD103UJ	796,00
1	Controladora Raid Adaptec ASR-5805Z 512MB 8-Port PCI-e	161,23
3	Interfaces de Rede Gigabit TP-LINK TG-3468 PCI-e	180,21
1	Fonte EVGA 600W 80 Plus 100-W1- 0600-KR	206,83
1	Gabinete Gamer V3X BLACK EDITION EN57417 Preto AEROCOOL	97,25
Total		3.518,41

Fonte: Autoria própria.

4.5 CONFIGURAÇÃO DE *HARDWARE* VIRTUAL DAS VMS NO AMBIENTE

Como já foi descrito no objetivo geral desse trabalho, o ambiente virtualizado de pequeno porte possui quatro máquinas virtuais, cada uma com os seguintes serviços: i) Servidor de banco de dados, ii) Controlador de domínio, diretório e servidor de arquivos, iii) Firewall e filtro de conteúdo web, iv) Servidor de aplicação web. A Tabela 6 mostra os requisitos recomendados de *hardware* para cada um dos serviços, e qual foi a configuração utilizada nas VMs. Devido as características dos testes que foram executados no ambiente, alguns recursos de *hardware* foram configurados nas VMs acima do recomendado.

Tabela 6 - Requisitos de hardware para cada serviço e hardware das VMs

Serviço	Escolhido	Hardware Recomendado	Hardware da VM
PDC	Microsoft Active Directory	CPU: 2 GHz ou mais Memória: 2 GB ou mais Espaço em disco: 40 GB Rede: 1 Interface	CPU: 4 núcleo 3.2 GHz Memória: 4 GB Disco: 300 GB Rede: 1 Interface
FIREWALL	PfSense	CPU: 1 GHz ou mais Memória: 1 GB Espaço em disco: 1 GB Rede: 2 Interface	CPU: 1 núcleo 3.2 GHz Memória: 1 GB Disco: 40 GB Rede: 3 Interface
SGBD	Microsoft Sql Server 2016	CPU: 2 GHz ou mais Memória: 4 GB ou mais Espaço em disco: 8 GB Rede: 1 Interface	CPU: 4 núcleo de 3.2 GHz Memória: 4 GB Disco: 300 GB Rede: 1 Interface
SERVIDOR APP	Apache, PHP, Mysql	CPU: 2 GHz ou mais Memória: 2 GB ou mais Espaço em disco: 30 GB Rede: 1 Interface	CPU: 2 núcleo 3.2 GHz Memória: 4 GB Disco: 100 GB Rede: 1 Interface

Fonte: Autoria própria.

Uma vez que o ambiente esteja configurado e as VMs instanciadas seguindo os passos do APÊNDICE A, o teste do ambiente pode ser realizado conforme descrito no próximo capítulo.

4.6 TESTES DE DESEMPENHO E RESULTADOS

Cada máquina virtual é considerada um ambiente de execução isolado das outras, mas que compartilha o conjunto de *hardware* do *host* físico. Em um ambiente de pequeno porte como o deste projeto, na qual não se tem vários *hosts* físicos para a distribuição da carga de trabalho, caso ocorra à sobrecarga de um VM, isso poderá degradar o desempenho do ambiente todo.

Considerando esse cenário, para testar o ambiente virtualizado é necessário colocar uma das VMs em condições de consumo excessivo de recursos como: cpu, memória, acesso a disco e tráfego de rede. E assim monitorar no ambiente do ESXI as informações de utilização desses recursos, e também verificar se os outros serviços executando nas outras VMs continuam funcionando sem perda de desempenho.

Para simular uma sobrecarga dos recursos de uma VM no ambiente desse projeto, foram utilizadas as seguintes ferramentas:

LoadStorm para CPU: Essa ferramenta permite configurar o número de *threads* e a carga aproximada em porcentagem para CPU, além de permitir configurar o tempo em minutos em que a carga será realizada.

Script VBScript para Memória: Esse *script* ao ser executado em uma VM, entra em um *loop* que vai gradativamente alocando a memória com um *array* de *strings*, até o limite de memória disponível.

IO Analyzer para leitura e escrita de disco: é uma ferramenta integrada, projetada para medir o desempenho de armazenamento em ambientes virtuais. Ela é distribuída em uma VM, tornando-a de fácil implantação no ambiente. O IO *analyzer* possui vários *presets* que representam a carga de trabalho que aplicações reais exerceriam em um dispositivo de armazenamento. Além disso ele trabalha integrado ao SDK da VMWare coletando as informações enquanto executa os testes, que depois podem ser visualizados em forma de relatórios.

iPerf 3 para tráfego de rede: A ferramenta permite realizar medições ativas da largura de banda máxima possível em redes IP. Ele suporta o ajuste de vários parâmetros relacionados ao TCP/UDP. Para cada teste, ele relata a largura de banda, a perda e outros parâmetros. Com essa ferramenta será possível gerar por

um período de tempo o tráfego limite que a interface de acesso aos serviços suporta e ver como o acesso aos outros serviços se comportarão.

4.6.1 SOBRECARGA DE CPU

No ambiente do ESXI a distribuição de carga de trabalho de CPU é feita pelo *scheduler* que entrega o processamento de acordo com a demanda da VM e de quantos núcleos virtuais foram atribuídos para ela. Por exemplo, se um host possui 4 processadores físicos *dual-core* executando 4 GHz cada, então o *host* terá 32 GHz disponível para ser distribuído entre as VMs (VMWARE, 2015).

Para testar o comportamento do ambiente virtualizado em uma condição de *stress* de CPU foi utilizada a VM que executa o serviço de PDC. Essa VM está configurada com 4 vCPU ou seja, utiliza todos os núcleos físicos disponíveis, 4 GB de memória e disco de 300GB com sistema operacional *Windows Server 2008 R2*.

Antes de começar os testes de sobrecarga da CPU, foram feitas as leituras da utilização de CPU no ambiente do ESXI e nas VMs (Tabela 7), e as duas informações mostram um estado de consumo mínimo de CPU.

Tabela 7 - Percentual de uso de CPU no ESXI e em cada VM antes do teste

LOCAL DA LEITURA	TIPO	SO	vCPUs	% USO CPU
ESXI	HOST	ESXI	4	1,00%
PDC-WIN-2K8-R2	VM	Windows Server 2008 R2	4	0,22%
FIREWALL-PFSENSE	VM	FreeBSD (64-bit)	1	0,19%
SGBD-SQLSERVER2016	VM	Windows Server 2012	4	0,31%
LAMP-SERVER	VM	Debian GNU/Linux 6 (64-bit)	2	0,07%

Fonte: Autoria própria.

Para simular a sobrecarga de CPU foi acessado o SO convidado da VM que foi utilizada para o teste, em seguida foi executada a ferramenta *LoadStorm*. A ferramenta foi configurada para utilizar 4 *threads* e um percentual de utilização de

CPU de 100%, uso de memória foi mantida em 0 (Figura 11), após essas configurações foi iniciado o teste de sobrecarga e mantido em execução.

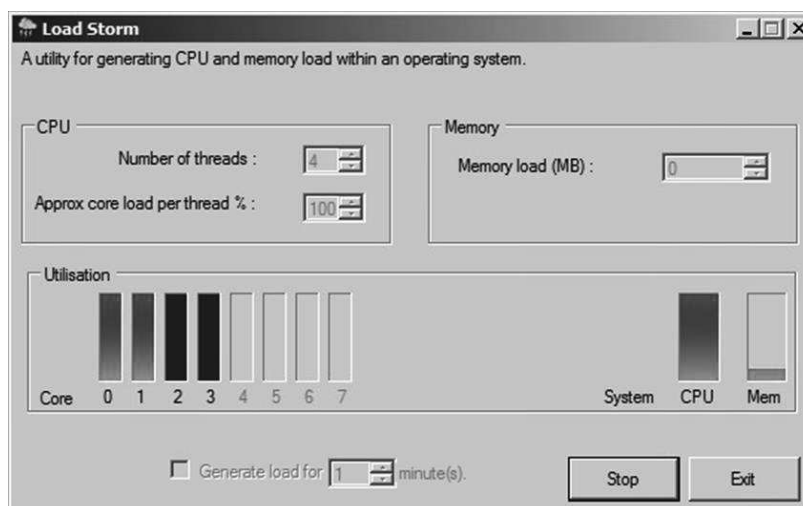


Figura 9 – Configuração e execução da ferramenta *LoadStorm*
Fonte: LoadStorm.

No período em que a carga de CPU estava executando, foram feitas novamente as leituras das informações de utilização de CPU do ESXI e das VMs (Tabela 8). O ESXI apresentou um gráfico de utilização de 100% de CPU, mas as operações no ambiente virtualizado por meio da interface de administração continuaram normais, permitindo realizar todas as funções. Já o serviço fornecido pela VM apresentou uma grande queda de desempenho, e as operações realizadas no SO da VM ficaram lentas.

Tabela 8 - Percentual de uso de CPU no ESXI e em cada VM durante o teste

LOCAL DA LEITURA	TIPO	SO	vCPUs	% USO CPU
ESXI	HOST	ESXI	4	100,00%
PDC-WIN-2K8-R2	VM	Windows Server 2008 R2	4	100,00%
FIREWALL-PFSENSE	VM	FreeBSD (64-bit)	1	0,10%
SGBD-SQLSERVER2016	VM	Windows Server 2012	4	0,25%
LAMP-SERVER	VM	Debian GNU/Linux 6 (64-bit)	2	0,37%

Fonte: Autoria própria.

O próximo passo foi verificar o desempenho dos serviços executando nas outras VMs, para isso foi utilizada a VM com o SGBD que também está configura com 4 vCPU e com Windows Server 2012 R2. Como pode ser visto na Tabela 8 essa VM está utilizando bem pouco recurso do CPU. Acessando o SO dessa VM, foram executadas algumas consultas e outras operações no ambiente, todas executaram sem apresentar quedas de desempenho.

Como os serviços nas outras VMs não apresentaram queda de desempenho, foi necessário sobrecarregar outra VM para verificar o comportamento do ambiente. Utilizando ainda a VM que executava o SGBD, foi iniciado a execução do *LoadStorm* e configurado quatro *threads* e um percentual de utilização de CPU de 40%, e colocado para executar ao mesmo tempo em que a outra VM estava sobrecarregada em 100%.

Após um período executando a sobrecarga da CPU de 100% na VM do PDC e 40% na VM do SGBD os seguintes resultados foram apresentados nas informações de utilização de CPU do EXSI e das VMs (Tabela 9).

Tabela 9 - Percentual de uso de CPU no ESXI e em cada VM durante os testes

LOCAL DA LEITURA	TIPO	SO	vCPUs	% USO CPU
ESXI	HOST	ESXI	4	96,00%
PDC-WIN-2K8-R2	VM	Windows Server 2008 R2	4	58,00%
FIREWALL-PFSENSE	VM	FreeBSD (64-bit)	1	0,17%
SGBD-SQLSERVER2016	VM	Windows Server 2012	4	40,00%
LAMP-SERVER	VM	Debian GNU/Linux 6 (64-bit)	2	0,09%

Fonte: Autoria própria.

As informações mostram um comportamento interessante do ESXI, ele não permitiu que a VM do PDC mesmo executando em 100% reservasse para si todo o uso do CPU físico. Pois a partir do momento que outra VM requisitou processamento ele distribuiu uma parte do processamento para a nova VM, diminuindo a quantidade disponível para a VM do PDC, por isso as operações realizadas nas outras VMs continuaram sem perda de desempenho.

Com isso fica claro que o ESXI trabalha com um sistema de isolamento das VMs para que uma não interfira na outra e compartilhe os recursos de hardware, e

mesmo com a sobrecarga de uma das VMs que tenha sido alocado todos os núcleos de CPU para ela, o ambiente virtualizado continuou operacional.

4.6.2 SOBRECARGA DA MEMÓRIA

O compartilhamento de memória no ESXI permite que as VMs sejam configuradas com mais memória do que a quantidade física disponível. Por exemplo, com 4 GB de memória física é possível instanciar 3 VMs com 2 GB de memória cada. Esses 2 GB configurados na criação da VM não serão alocados exclusivamente para cada VM, esse valor só representa o limite que o SO hóspede executando na VM terá disponível. Então no momento em que a VM solicitar uso de memória é que realmente o ESXI aloca para VM, mas somente a quantidade requisitada, deixando o restante para ser compartilhada com as outras VMs (VMWARE, 2009).

Tendo em vista o exemplo anterior, enquanto as VMs estiverem usando a memória de forma moderada o ESXI fará a distribuição de acordo com a demanda, mantendo um bom desempenho das VMs. Se acontecer de todas as 3 VMs tiverem sobrecarga do uso de memória, todo o ambiente virtualizado poderá ser comprometido, pois o ESXI não terá memória física para todas as VMs.

No ambiente que será realizado os testes de sobrecarga de memória, estão disponíveis 16 GB de memória física. Para simular a situação em que as VMs requisitam mais memória do que a disponível foi feita uma modificação na quantidade de memória de uma das VMs de 4 GB para 15 GB. A soma total da memória configurada para todas as VMs ficou em 21 GB, a distribuição é mostrada abaixo:

- ✓ 1 VM com 15 GB de memória (PDC).
- ✓ 1 VM com 4 GB de memória (SGBD).
- ✓ 1 VM com 1 GB de memória (*Firewall*).
- ✓ 1 VM com 4 GB de memória (Servidor Web).

Para verificar as condições de uso de memória no ambiente virtualizado as seguintes métricas estão disponíveis: fazer a leitura do próprio SO convidado ou no

ambiente do ESXI. No ESXI as duas informações principais são, *consumed host memory* que representa a quantidade de memória atribuída para a VMs, e *active guest memory* que é a quantidade de memória que está sendo usada atualmente pelo sistema operacional convidado e seus aplicativos (VMWARE, 2009).

No ambiente virtualizado, o ESXI trabalha interceptando as instruções vindas do SO convidado das VMs como acesso a disco, alocação de memória e CPU etc. Então quando o SO solicita uso de memória o ESXI intercepta essa requisição e faz a correta alocação na memória física e consegue registrar essa informação nas métricas de memória, mas quando o SO desaloca porções da memória nenhuma instrução é passada para o ESXI mantendo as métricas com informações desatualizadas (VMWARE, 2009).

Com base nessas informações é possível concluir que as métricas do ESXI não são confiáveis para verificação da quantidade de memória em uso. A melhor forma de verificar a quantidade de memória em uso em determinado momento é verificar diretamente nos SOs convidados das VMs.

Para seguir com os testes, primeiramente foram iniciadas todas as VMs e verificado em cada SO convidado quanto de memória física cada uma estava usando, a Tabela 10 mostra que a memória usada por cada VM ainda está em uma situação normal.

Tabela 10 - Informações de memória nos SOs convidados antes da sobrecarga				
VMs	Sistema Operacional	Configurada	Em uso	Livre
PDC-WIN-2K8-R2	Windows Server 2008 R2	15 GB	1093 MB	13895 MB
FIREWALL-PFSENSE	FreeBSD	1 GB	241 MB	783 MB
SGBD-SQLSERVER2016	Windows Server 2012 R2	4 GB	1967 MB	2103 MB
LAMP-SERVER	Debian	4 GB	472 MB	3492 MB

Fonte: A autoria própria.

Em seguida foi executado o *script* de sobrecarga na VM com 15 GB de memória, após um tempo de execução o uso de memória do SO hospedeiro chegou ao seu limite (Figura 10), e então foi feita uma nova coleta das informações de memória dos SOs de todas as VMs (Tabela 11).

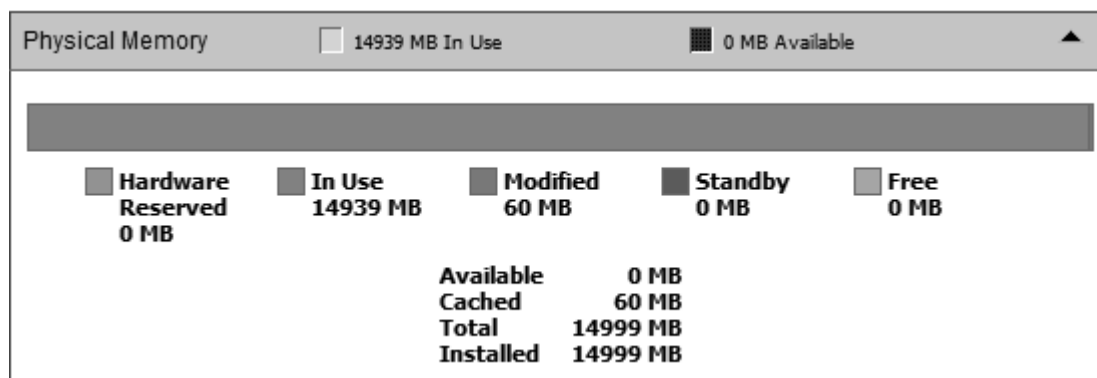


Figura 10 – Leitura de memória no SO convidado após a sobrecarga

Fonte: Microsoft Windows Server 2008 R2

Tabela 11 - Informações de memória nos SOs convidados durante a sobrecarga

VMs	Sistema Operacional	Configurada	Em uso	Livre
PDC-WIN-2K8-R2	Windows Server 2008 R2	15 GB	14939 MB	0 MB
FIREWALL-PFSENSE	FreeBSD	1 GB	725 MB	299 MB
SGBD-SQLSERVER2016	Windows Server 2012 R2	4 GB	3925 MB	179 MB
LAMP-SERVER	Debian	4 GB	3067 MB	898 MB

Fonte: Autoria própria.

Os dados de utilização de memória das VMs na Tabela 11, mostram que a sobrecarga da VM com o serviço de PDC com 15 GB de memória afetou o uso de memória das outras VMs. Os SOs convidados das outras VMs identificaram que não tinham memória física disponível para elas e assim ficaram também sobrecarregas.

O passo seguinte foi verificar o estado do ambiente virtualizado e dos serviços executando nas outras VMs. O ambiente de gerenciamento ficou com desempenho ruim, mas permitiu realizar várias operações, como criação de VMs, importação, edição das VMs, etc. Já os serviços das VMs ficaram com desempenho extremamente ruins, uma consulta no SQL Server que durava 2 segundos, passou para 1 minuto e 30 segundos, a abertura de uma página no servidor web também ficou lenta no primeiro acesso, e várias outras operações realizadas nos SOs convidados das VMs ficaram comprometidas.

4.6.3 SOBRECARGA DO ACESSO A DISCO

Para um melhor desempenho e redundância, o ambiente virtualizado desse projeto possui 4 discos SATA II de 7200 RPM configurados em RAID 10 para armazenamento das VMs. O arranjo faz primeiramente o espelhamento entre dois discos e depois faz a segmentação (Figura 11). Além disso o ESXI está instalado em um HD SSD de 120 GB. Segundo a SAMSUNG, fabricante dos discos utilizados no RAID, o *average seek time*, tempo que a cabeça de leitura e gravação leva para encontrar a localização física de um determinado dado, é de 8.9 ms. E a média de latência (*average latency*), tempo para a cabeça ser posicionada no setor correspondente, é de 4.17 ms (Figura 12).

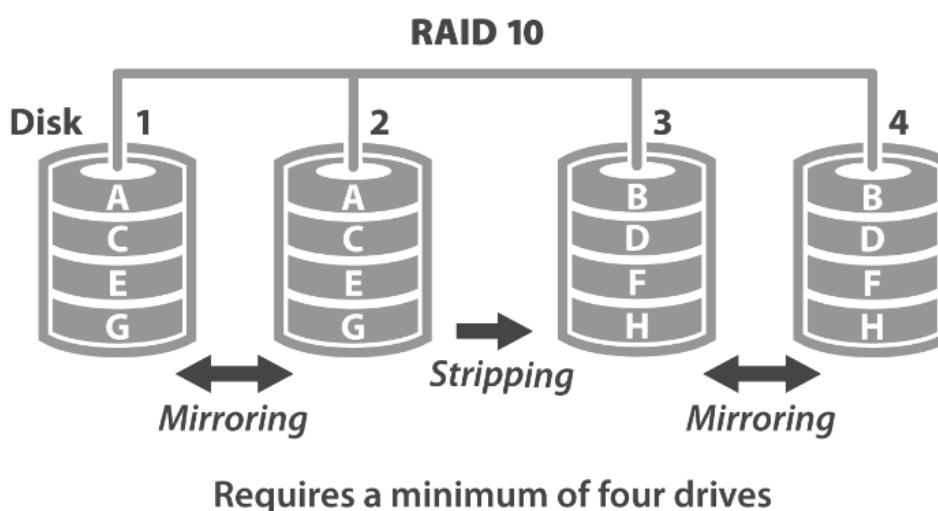


Figura 11 – Configuração dos discos no RAID 10

Fonte: <http://www.thecloudcalculator.com/calculators/disk-raid-and-iops.html>

PERFORMANCE SPECIFICATIONS	
Average Seek time (typical)	8.9 ms
Average Latency	4.17 ms
Data Transfer Rate	
Media to/from Buffer (Max.)	175 MB/sec
Buffer to/from Host (Max.)	300 MB/sec
Drive Ready Time (typical)	160~320GB 8 sec
	500~640GB 12 sec
	750~1000GB

Figura 12 – Informação de tempo de busca e latência de cada disco

Fonte: <https://www.samsung.com>

Com esses dados é possível calcular o número teórico de IOPS de cada disco, utilizando a fórmula $IOPS = 1 / (average\ latency\ seconds + average\ seek\ time\ seconds)$ disponibilizada por MARCO BROEKEN em seu site vClouds, o seguinte resultado é obtido: $1 / ((8.9 + 4.17) / 1000) = 76,51$ IOPS, em um ambiente real a média fica em 88 IOPS. Caso o projeto fosse configurado em RAID 0, o total de IOPS seria a multiplicação do valor obtido do cálculo de um disco por 4.

Utilizando RAID 10 tem-se um ganho de desempenho nas operações de leitura, mas também um pouco de perda nas operações de escrita devido a redundância dos dados. Então variando o percentual de operações de escrita e leitura os IOPS também irão variar. Com uma calculadora de IOPS para configurações em RAID disponibilizado por JEREMY CHIVERS em seu site MY VMWARE BLOG, é possível especificar a configuração de RAID em que os discos estão, e fazer variações nos valores de leitura e escrita sequencial ou aleatória e obter o total de IOPS teórico, os resultados para algumas variações podem ser vistos na Tabela 12.

Tabela 12 - IOPS para taxas de leituras e escritas diferentes em RAID 10

% LEITURA	% ESCRITA	IOPS
100	0	350
0	100	175
50	50	263

Fonte: A autoria própria.

Em um ambiente virtualizado geralmente o que causa perda de desempenho nos dispositivos de armazenamento é a alta latência de operações de entrada e saída. Uma latência com valor acima de 20 ou 30 milissegundos poderão causar problemas de desempenho (DIECKHANS, 2012).

Para sobrecarregar os dispositivos de armazenamento do ambiente virtualizado, foram executados alguns testes com a ferramenta *IO Analyzer* da VMWare. Esses testes são baseados em *presets* que são configurados para simular a sobrecarga de determinadas aplicações como: sql server, web server ou uma operação de escrita e leitura de dados. A Tabela 13 mostra quais testes foram

executados no ambiente, assim como o percentual de operações de escrita e leitura, tamanho do bloco de dados que a aplicação utiliza e o percentual de operações sequenciais e aleatórias.

Tabela 13 - Testes executados com o IO Analyzer

TESTES	BLOCO	% LEITURA	% ESCRITA	% SEQ.	% ALEAT.	DUR. MIN
1 - Web Server	8K	95	5	25	75	10
2 - Sql Server	64K	66	34	0	100	10
3 - Leitura Aleatória	512K	100	0	0	100	10
4 - Leitura Sequencial	512K	100	0	100	0	40
5 - Escrita Aleatória	512K	0	100	0	100	40
6 - Escrita Sequencial	512K	0	100	100	0	10

Fonte: Autoria própria.

Após a execução de cada teste foi possível visualizar no *IO Analyzer* a informação de latência das operações de entrada e saída, e também o número máximo de operações de entrada e saída que o ambiente conseguiu trabalhar durante cada um dos testes.

Enquanto cada teste era executado, foram verificados se os serviços em cada VM apresentavam alguma perda de desempenho. E para visualizar melhor o quanto cada teste de sobrecarga estava impactando o ambiente foi realizado uma operação de leitura e outra de escrita de um arquivo de 1 GB no mesmo dispositivo que estava sobrecarregado. Assim foi possível comparar o tempo gasto das operações no momento de cada teste.

A operação de escrita ou leitura do arquivo de 1 GB no ambiente sem nenhuma sobrecarga durou 14 segundos cada operação. Esse valor foi usado como controle para comparar com os resultados das mesmas operações no ambiente sobrecarregado. Cada teste foi executado três vezes e feito a média dos valores obtidos. Os resultados dos testes são mostrados na Tabela 14, a coluna TESTES mostra o nome do teste, IOPS é a média de IOPS que foi possível atingir em cada teste, LATÊNCIA é o valor médio em milissegundos em que o dispositivo de armazenamento atingiu, ESCRITA 1 GB mostra o tempo que levou para realizar essa operação ao mesmo tempo em que se executava o teste, LEITURA 1 GB o

mesmo da coluna anterior só mudando a operação, SERVIÇOS VMS mostra a situação das VMs e os serviços executados por elas durante cada teste.

Tabela 14 - Resultado dos testes de acesso a disco

TESTES	\bar{X} IOPS	\bar{X} LATÊNCIA	\bar{X} ESCRITA 1GB	\bar{X} LEITURA 1GB	SERVIÇOS VMS
1 - Web Server	343,50	12,81 ms	1m23s	21s	Normais
2 - Sql Server	248,23	68,92 ms	4m45s	1m6s	Leve <i>delay</i> I/O
3 - Leitura Aleatória	180,77	94,66 ms	4m05s	1m43s	Leve <i>delay</i> I/O
4 - Leitura Sequencial	502,84	36,57 ms	35m01s	18s	Leve <i>delay</i> I/O
5 - Escrita Aleatória	72,30	263,90 ms	28m24s	1m20s	Leve <i>delay</i> I/O
6 - Escrita Sequencial	277,99	61,71 ms	7m44s	20s	Leve <i>delay</i> I/O

Fonte: Autoria própria.

Observando os resultados dos testes, é possível ver uma variação do número de IOPS atingido em cada teste e o que foi calculado na Tabela 12, mas isso já era esperado, pois os cálculos mostram valores que teoricamente o dispositivo de armazenamento atingiria. Além disso cada teste fez com que a latência do dispositivo aumentasse impactando no desempenho de outras operações no ambiente principalmente de escrita, com exceção do teste 1 que manteve a latência baixa, porém o teste 4 devido à natureza da operação sequencial o número de IOPS ficou elevado e criou um gargalo nas operações de escrita.

Quanto ao desempenho dos serviços das VMs, somente o primeiro teste que simula sobrecarga de um servidor web é que permitiu realizar as operações sem perda de desempenho. Para os outros testes os serviços continuaram executando, mas quando alguma operação de leitura ou escrita em disco era requisitada, por exemplo, abertura de um programa, ou página web, foi possível notar um *delay* nessas operações, mas que não comprometeu a execução.

O maior impacto realmente foi realizar a operação de escrita de um arquivo de 1 GB no disco ao mesmo tempo em que os testes eram realizados, para todos os testes apresentou um aumento no tempo comparado aos 14 segundos que essa operação levou quando o ambiente não estava sobrecarregado. Os testes 4 e 5 foram os que mais impactaram nessa operação fazendo com que a escrita do arquivo durasse 35min01s e 28min24s respectivamente.

A operação de leitura do arquivo de 1 GB ao mesmo tempo que se executava os testes não foi muito impactada, com exceção dos testes 2, 3 e 5 que resultou em um leve aumento no tempo dessa operação.

4.6.4 SOBRECARGA DO TRÁFEGO DE REDE

Em um ambiente como o desse projeto, não se utilizam interfaces de rede de alta velocidade, pois devido as baixas taxas de transferência espera-se que não ocorra sobrecarga nas mesmas. Além disso internamente ao ESXI todas as VMs estão ligadas ao vSwitch0 e esse por sua vez ligado a uma única interface física (Figura 13). Essa organização também é mostrada em mais detalhes na Figura 14.

A Figura 14 mostra que o ambiente possui 4 interfaces físicas, cada uma delas está associada a um vSwitch. O vSwitch0 é o que faz *uplink* com a interface que está ligada no switch físico da rede da empresa, e todas as VMs possuem uma interface virtual ligada no vSwitch0 para fornecer os serviços. A VM com o serviço de *firewall* possui mais 2 interfaces além da que está ligada no vSwitch0, uma ligada ao vSwitch1 e a outra ao vSwitch2, e esses por sua vez ligados a interfaces físicas conectadas a dois *links* de internet para ter redundância no ambiente. O vSwitch3 e a interface física na qual ele está ligado é utilizado como reserva, para o caso de precisar ser feita alguma configuração diferente no ambiente.

Nesse cenário todos os serviços fornecidos pelas VMs são acessados por uma única interface de rede física de 1 *gigabit*.

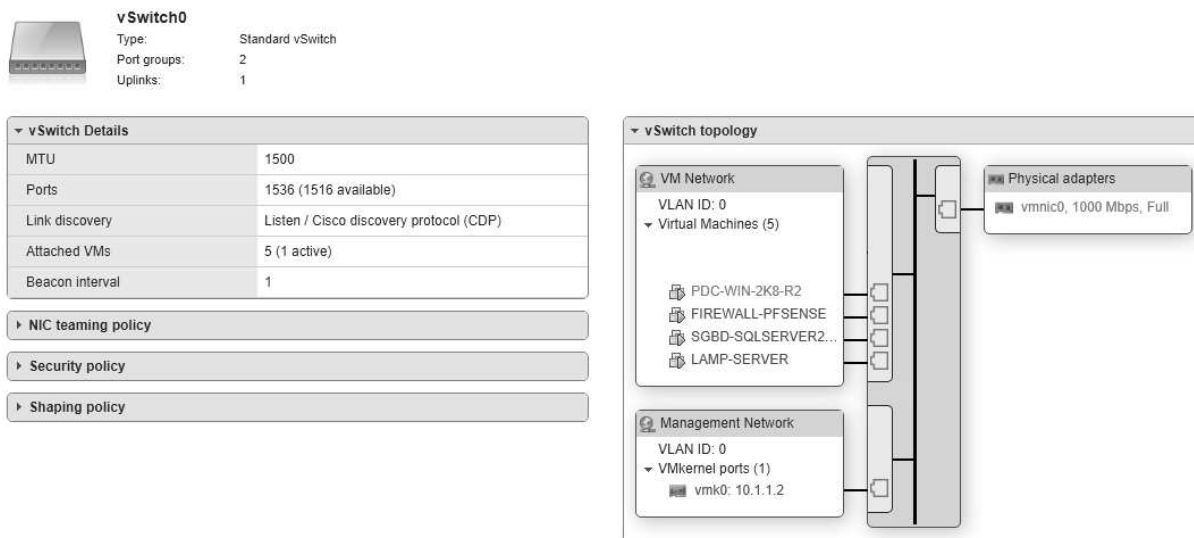


Figura 13 – VMs ligadas em um mesmo vSwitch e uma interface física
 Fonte: *Web Client ESXI*

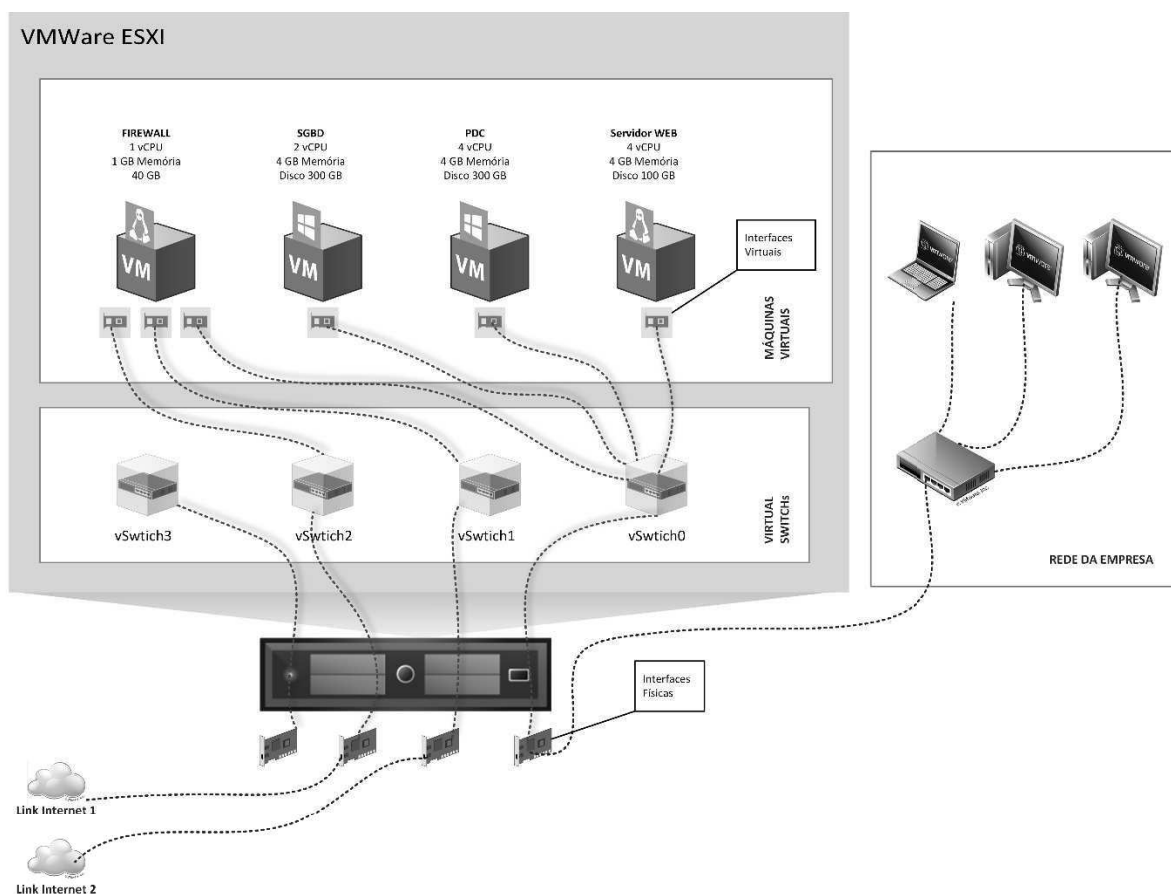


Figura 14 – Organização da rede virtual e física no ambiente do ESXI
 Fonte: *Adaptação de VMware Visio stencils*

Os testes que foram executados a seguir são justamente para simular uma condição de tráfego intenso entre uma das VMs e uma estação qualquer da rede física, e assim verificar a condição dos outros serviços que são fornecidos por essa mesma interface de rede.

Para começar os testes foi iniciado o *IPerf* como servidor em uma VM com o seguinte comando: `iperf.exe -s -P 10 -p 5001 -w 64K`.

-s: IPerf inicia como servidor.

-P 10: Inicia 10 conexões em paralelo.

- p 5001: A porta que escutará as conexões é a 5001.

-w 64K: Tamanho da janela do protocolo TCP, 64K é o padrão.

Iniciado o servidor, foi utilizado uma estação de trabalho como cliente, essa estação possui uma interface de rede de 1 *gigabit* e está ligada na mesma rede física que a o servidor ESXI. Na estação foi executado o seguinte comando do IPerf: `iperf.exe -c 10.1.1.3 -P 10 -p 5001 -w 64K -t 600`.

-c 10.1.1.3: IPerf para inicia como cliente e conecta-se no ip 10.1.1.3.

-P 10: Criar 10 conexões paralelas.

-w 64K: Usar tamanho de janela de 64K.

-t 600: Executar o teste durante 600 segundos.

Durante a execução do teste foram coletadas informações no ESXI (Figura 15) para ver o tráfego que estava sendo gerado na interface física do ESXI e no vSwitch a qual VM estava conectada. Em destaque é possível ver que na interface física `vmnic0` o tráfego foi de 910 Mbps e no vSwitch 913 Mbps, ficando próximo do limite da interface que é de 1000 Mbps ou 1 Gbps.

10.1.1.2 - PuTTY
2:45:27pm up 2:36, 494 worlds, 4 VMs, 13 vCPUs; CPU load average: 0.01, 0.08, 0.10

DNAME	PORT-ID	USED-BY	TEAM-PNIC	PKTIX/s	MbTX/s	PS2TX	PKTRX/s	MbRX/s	PSZRZ	%DRPTX	%DRPRX
vSwitch0	33554433	Management	n/a	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
vSwitch0	33554434	vmnic0		30657.09	14.56	62.00	81944.06	910.81	1456.00	0.00	0.00
vSwitch0	33554435	Shadow of vmnic0	n/a	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
vSwitch0	33554436	vmk0	vmnic0	383.65	0.70	239.00	52.32	0.03	79.00	0.00	0.00
vSwitch0	33554437	67703:FIREWALL-PFSENSE	vmnic0	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
vSwitch0	33554438	67849:PDC-WIN-2K8-R2	vmnic0	30378.07	13.91	60.00	81874.30	913.25	1462.00	0.00	0.00
vSwitch0	33554439	67987:SGBD-SQLSERVER2016	vmnic0	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
vSwitch0	33554440	68139:LAMP-SERVER	vmnic0	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
vSwitch1	50331649	Management	n/a	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
vSwitch1	50331650	vmnic1	-	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
vSwitch1	50331651	Shadow of vmnic1	n/a	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
vSwitch1	50331652	67703:FIREWALL-PFSENSE	vmnic1	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
vSwitch2	67108865	Management	n/a	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
vSwitch2	67108866	vmnic2	-	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
vSwitch2	67108867	Shadow of vmnic2	n/a	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
vSwitch2	67108868	67703:FIREWALL-PFSENSE	fallback	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
vSwitch3	83886081	Management	n/a	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
vSwitch3	83886082	vmnic3	-	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
vSwitch3	83886083	Shadow of vmnic3	n/a	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00

Figura 15 – Tráfego de rede em uma VM e na interface física do ESXI
Fonte: Esxtop Console ESXI

Ainda com o teste em execução foram verificados os serviços da VM que sofria sobrecarga e das outras VMs e todas continuaram funcionando sem apresentar queda desempenho quando executados comandos na rede. Para visualizar melhor o que acontece quando outras VMs trafegavam informações na rede durante o teste, foi iniciado o servidor do *IPerf* em outra VM. E a partir de outra estação com uma interface de rede de 100 Mbps foi iniciado o *IPerf* para gerar esse tráfego nessa outra VM, o resultado é apresentado na Figura 16.

10.1.1.2 - PuTTY
9:26:57pm up 4:19, 498 worlds, 4 VMs, 13 vCPUs; CPU load average: 0.01, 0.01, 0.01

USED-BY	TEAM-PNIC	DNAME	PKTIX/s	MbTX/s	PS2TX	PKTRX/s	MbRX/s	PSZRZ	%DRPTX	%DRPRX
Management	n/a	vSwitch0	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
vmnic0	-	vSwitch0	39321.00	18.63	62.00	83539.18	921.84	1446.00	0.00	0.00
Shadow of vmnic0	n/a	vSwitch0	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
vmk0	vmnic0	vSwitch0	301.59	0.77	336.00	71.81	0.04	72.00	0.00	0.00
67716:FIREWALL-PFSENSE	vmnic0	vSwitch0	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
67923:PDC-WIN-2K8-R2	vmnic0	vSwitch0	34912.11	15.98	60.00	75224.03	834.84	1454.00	0.00	0.00
68130:SGBD-SQLSERVER2016	vmnic0	vSwitch0	4092.95	1.87	60.00	8257.70	89.66	1423.00	0.00	0.00
68328:LAMP-SERVER	vmnic0	vSwitch0	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Management	n/a	vSwitch1	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
vmnic1	-	vSwitch1	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Shadow of vmnic1	n/a	vSwitch1	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
67716:FIREWALL-PFSENSE	vmnic1	vSwitch1	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Management	n/a	vSwitch2	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
vmnic2	-	vSwitch2	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Shadow of vmnic2	n/a	vSwitch2	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
67716:FIREWALL-PFSENSE	fallback	vSwitch2	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Management	n/a	vSwitch3	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
vmnic3	-	vSwitch3	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Shadow of vmnic3	n/a	vSwitch3	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00

Figura 16 – Tráfego de rede em duas VM e na interface física do ESXI
Fonte: Esxtop Console ESXI

Os resultados na Figura 16 mostram o porquê das outras VMs continuarem com os serviços normais, observando em destaque as 2 VMs sobrecarregadas utilizaram cada uma parte da banda disponível no canal de comunicação, que somados dá aproximadamente o total utilizado na interface vmnic0. Esses mesmos

testes realizados com o protocolo TCP, também foram realizados com UDP e o mesmo comportamento foi observado.

Considerando o resultado desses testes, a cada conexão criada com o servidor ESXI, a largura de banda é dividida entre as conexões. E como os serviços das outras VMs não precisam de tráfego elevado para fornecerem seus serviços fica imperceptível. Obviamente que, se o número de estações utilizando toda a largura de banda for muito grande, chegará o momento em que a largura de banda reservada para cada uma será mínima. Assim, qualquer operação na rede por mais simples que seja terá seu desempenho comprometido. Para exemplificar, caso a rede possua 20 estações, cada uma com conexões fazendo uso de toda a banda disponível, o acesso ao servidor do ESXI para cada uma ainda seria de 50 Mbps, pois seria 1000 Mbps da interface física dividido por 20.

4.6.5 COMPARATIVO DOS TESTES REALIZADOS E DISCUSSÕES

Fazendo um resumo dos testes realizados foi possível elaborar a Tabela 15, que mostra o teste de cada recurso de *hardware*, e se impactou o desempenho do ambiente virtualizado, VM sobrecarregada e serviços em outras VMs.

Tabela 15 - Resumo dos testes de sobrecarga do ambiente virtualizado

Recurso testado	Tipo do teste	Desempenho ESXI	Desempenho na VM objeto do teste	Desempenho nas outras VMs
CPU	Sobrecarga dos 4 núcleos de CPU em uma VM.	Normal, permitindo todas as operações.	Ruim.	Normal, conforme a demanda o ESXI distribuiu a carga.
MEMÓRIA	Utilização de mais memória do que o disponível.	Ruim, mas permitiu todas as operações.	Ruim.	Ruim.
DISCO	Operações de escrita e leitura, simulando aplicações.	Normal, mas operações de leitura e escrita ruins.	-	Operações de leitura e escrita ruins.
REDE	Gerar alto tráfego de dados na interface que fornece os serviços.	Normal, precisa de várias estações acessando para comprometer.	Normal, precisa de várias estações acessando para comprometer.	Normal, precisa de várias estações acessando para comprometer.

Fonte: Autoria própria.

Para cada recurso de *hardware* testado, eles foram colocados em uma condição extrema que na maioria das vezes não acontecerá em um ambiente de produção. No entanto serviu para entender como o ambiente virtualizado realmente funciona compartilhando seus recursos entre as VMs.

Muitas vezes o ambiente é comprometido por uma má configuração na distribuição dos recursos de *hardware*. Uma boa prática na consolidação de servidores para um ambiente virtual, é a de não configurar as VMs com mais recursos do que ela realmente precisará, ou seja, configura-se com o mínimo recomendado e vai aumentando conforme a demanda. Essa situação pode ser vista durante os testes de memória, em que mais memória foi alocada para as VMs do que existia disponível.

Um aspecto importante é que serviços instalados em *hardware* físico, assim como em ambiente virtual, precisam ser monitorados. Outra boa prática é a utilização de ferramentas que mostrem a condição de consumo de cada recurso, e que permita a configuração de gatilhos que gerem alertas por email ou SMS em caso de algum recurso ultrapasse seus limites de uso.

5 CONCLUSÃO

Por meio deste trabalho foi realizada a avaliação de diferentes cenários críticos no ambiente virtualizado, que em um cenário de uma pequena empresa poderiam não ocorrer, ou seriam identificados antes que prejudicassem o desempenho de todos os outros serviços em execução. Porém por se tratar de um ambiente de pequeno porte, e que precisava ser validado, os testes realizados foram necessários.

Os resultados dos testes demonstraram que a utilização de memória acima do total físico disponível, e algumas operações de acesso a disco, seriam os recursos que facilmente poderiam comprometer desempenho do ambiente. Para evitar esses problemas, a memória teria que ser dimensionada entre as VMs somente até o limite físico disponível, ou aumentar a sua quantidade física. Já o acesso a disco, com a utilização de um *storage* dedicado ou um arranjo em RAID com mais discos distribuiria a sobrecarga das operações.

Por outro lado, o trabalho também demonstrou como as pequenas empresas podem tirar proveito dos benefícios da virtualização, utilizando um conjunto de hardware de baixo custo e ferramentas gratuitas. Além disso, o guia de instalação e configuração básica do VMWare ESXI, servirá de guia para a empresa começar a utilizar a virtualização.

No entanto, quando se trata de ambiente virtualizado, é preciso considerar a redundância do ambiente e tolerância a falhas para manter a continuidade dos serviços. Tendo em vista que esses fatores não foram tratados nesse trabalho, fica a possibilidade de pesquisas futuras que trabalhem essas questões, mas ainda mantendo o foco no cenário de pequeno porte e utilização de ferramentas gratuitas.

REFERÊNCIAS

CABRAL, C. C. **Licenciamento do XenServer**. Disponível em: < <http://cleriston.com.br/post/110423732213/licenciamento-do-xenserver> >. Acesso em: 13 ago. 2017.

CARISSIMI, Alexandre. **Virtualização: da teoria a soluções**. Rio Grande do Sul: GTA/UFRJ, 2008. Cap. 4. Disponível em: < <http://www.gta.ufrj.br/ensino/CPE758/artigos-basicos/cap4-v2.pdf> >. Acesso em: 01 jun. 2017.

CITRIX. **XenServer 7.2 Configuration Limits**. Disponível em: < <https://docs.citrix.com/content/dam/docs/en-us/xenserver/current-release/downloads/xenserver-config-limits.pdf> >. Acesso em: 13 ago. 2017.

ESX VIRTUALIZATION. **Esxi free vs paid – what are the differences?** Disponível em: < <https://www.vladan.fr/esxi-free-vs-paid/> >. Acessado em: 13 ago. 2017.

FERNANDES, Aguinaldo A.; DE ABREU, Vladimir F. **Implantando a Governança de TI**. 4ª. ed. Rio de Janeiro: Brasport, 2014.

GARTNER. **Magic quadrant for x86 server virtualization infrastructure**. Disponível em: < <https://www.gartner.com/doc/reprints?ct=160707&id=1-3B9FAM0&st=sb> >. Acessado em: 14 set. 2017.

LAUREANO, Marcos. **Máquinas Virtuais e Emuladores: Conceitos técnicas e aplicações**. São Paulo: Novatec, 2006.

OLIVEIRA, G. L. C. D. **Descubra o Hyper-V Server 2016**. Disponível em: < <http://cooperati.com.br/2017/08/31/descubra-o-hyper-v-server-2016/> >. Acessado em: 13 ago. 2017.

MANIK, Varun Kumar; ARORA, Deepak. **Performance Comparison of Commercial VMM: ESXI, XEN, HYPER-V & KVM**. Lucknow, India: Department of Computer Science & Engineering, Amity University, 2016.

MARSHALL, David; REYNOLDS, Wade A.; MCCRORY, Dave. **ADVANCED SERVER VIRTUALIZATION VMware and Microsoft Platforms in the Virtual Data Center**. Boca Raton, NY, US: Auerbach Publications, 2006.

MATTOS, Diogo M. F. **Virtualização: VMware e Xen**. Rio de Janeiro: GTA/UFRJ, 2009. Disponível em: < http://www.gta.ufrj.br/grad/08_1/virtual/artigo.pdf >. Acesso em: 28 mai. 2017.

MAURER, Thomas. **What's new in windows server 2016 hyper-v**. Disponível em: < <https://www.thomasmaurer.ch/2015/05/whats-new-in-windows-server-2016-hyper-v/> >. Acessado em: 13 ago. 2017.

MICROSOFT. **Windows Server 2016 Hyper-V large-scale VM performance for in-memory transaction processing**. Disponível em: <<https://blogs.technet.microsoft.com/windowsserver/2016/09/28/windows-server-2016-hyper-v-large-scale-vm-performance-for-in-memory-transaction-processing/>>. Acesso em: 13 ago. 2017.

MY VMWARE BLOG. **IOPS Calculator**. Disponível em: < <http://www.myvmwareblog.com/2012/12/29/iops-calculator-2/> >. Acessado em: 14 ago. 2017.

POLAST, Budhprakash; BHATIA, Anupam; BHATHAL, Gurjeet Singh. **A comparative study of Various Hypervisors Performance**. International Journal of Scientific & Engineering Research, Volume 7, ed. 12, dez. 2016. Disponível em: < <https://www.ijser.org/researchpaper/A-comparative-study-of-Various-Hypervisors-Performance.pdf> >. Acessado em: 14 nov. 2017.

POLLON, Vanderlei. **Virtualização de servidores em ambientes heterogêneos distribuídos – estudo de caso**. Rio Grande do Sul: UFRJ, 2008. Disponível em: < <http://www.lume.ufrgs.br/bitstream/handle/10183/15988/000695318.pdf> >. Acesso em: 02 jun. 2017.

SERUYA, Francisco C. L. e T. **A virtualização como factor multiplicador da competitividade e eficiência das organizações**. Dissertação de Mestrado em Gestão. Universidade Lusíada de Lisboa, 2013. Disponível em: < http://repositorio.ulusiada.pt/bitstream/11067/783/1/mg_francisco_seruya_dissertacao.pdf >. Acesso em: 02 jun. 2017.

VLOUDS VIRTUALIZATION CHANGES EVERYTHING. **Calculate iops**. Disponível em: < <http://www.vclouds.nl/calculate-iops/> >. Acessado em: 14 ago. 2017.

VERAS, Manoel. **VIRTUALIZAÇÃO Tecnologia Central do Datacenter**. 2. ed. Rio de Janeiro: Brasport Editora, 2016.

VMWARE. **The cpu scheduler in vmware vsphere 5.1**. Disponível em: < <https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/vmware-vsphere-cpu-sched-performance-white-paper.pdf> >. Acessado em: 15 ago. 2017.

VMWARE. **Understanding memory resource management in vmware esx server.** Disponível em: < https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/perf-vsphere-memory_management.pdf >. Acessado em: 15 ago. 2017.

VMWARE. **Vmware infrastructure architecture overview.** Disponível em: < https://www.vmware.com/pdf/vi_architecture_wp.pdf >. Acessado em: 14 ago. 2017.

VMWARE. **Vsphere hypervisor.** Disponível em: < <https://www.vmware.com/products/vsphere-hypervisor.html> >. Acessado em: 13 ago. 2017.

APÊNDICE A – INSTALAÇÃO E CONFIGURAÇÃO DO VMWARE ESXI 6.5

A.1 REQUERIMENTOS DE HARDWARE PARA O ESXI 6.5

Para a instalação do ESXI 6.5 é preciso que os requerimentos mínimos de hardware e recursos listados abaixo sejam atendidos:

- ✓ Um servidor ou conjunto de hardware que de preferência esteja na HCL (*Hardware Compatibility List*) da VMWare, disponível em: <http://www.vmware.com/resources/compatibility>.
- ✓ Processador de 64 bits com 2 núcleos e com suporte a virtualização por hardware. Esse recurso deve estar habilitado no bios (Intel VT-x ou AMD RVI).
- ✓ Recurso NX/XD habilitado no bios do *host*.
- ✓ 1 ou mais interfaces de rede gigabit, podem ser consultados na lista de compatibilidade.
- ✓ 1 disco local SATA ou SCSI com 5.2 GB livre para instalação do ESXI, e outro disco local SATA ou SCSI para armazenamento das VMs.

A.2 OBTENDO O INSTALADOR DO ESXI 6.5 E A LICENÇA GRATUÍTA

Primeiramente é necessário acessar o site <https://my.vmware.com/web/vmware/login> e criar uma conta para ter acesso aos downloads caso ainda não tenha a conta. Acessando o endereço será apresentado a página da Figura A.1, basta clicar em **Register**, e na próxima tela preencher com os dados solicitados, concordar com os termos e clicar na opção **Continue**. Após isso será enviado uma email para o endereço informado, para finalizar o cadastro é necessário acessar a conta de email e seguir as instruções para fazer a ativação do cadastro.



Figura A.1 – Site para login e criação da conta no My VMWare

Com a conta criada, seguir para o endereço <https://www.vmware.com/br.html>, e clicar em **PRODUTOS** (Figura A.2) e depois em **vSphere Hypervisor** na seção produtos gratuitos (Figura A.3).

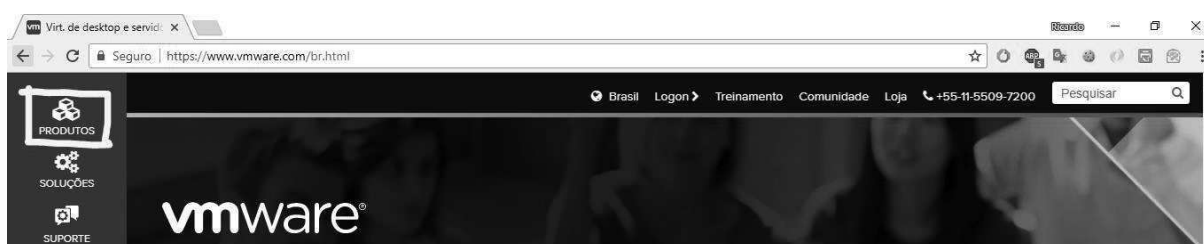


Figura A.2 – Seção de PRODUTOS VMWare



Figura A.3 – Opção vSphere Hypervisor em produtos gratuitos

Na próxima tela (Figura A.4) clicar em **Fazer download agora**, caso não tenha entrado com a conta criada anteriormente, será solicitado que entre com email e senha informados no momento do registro da conta. Ao entrar com o email e senha ou se já estiver logado a tela da Figura A.5 será exibida.



Figura A.4 – Opção para download do ESXI

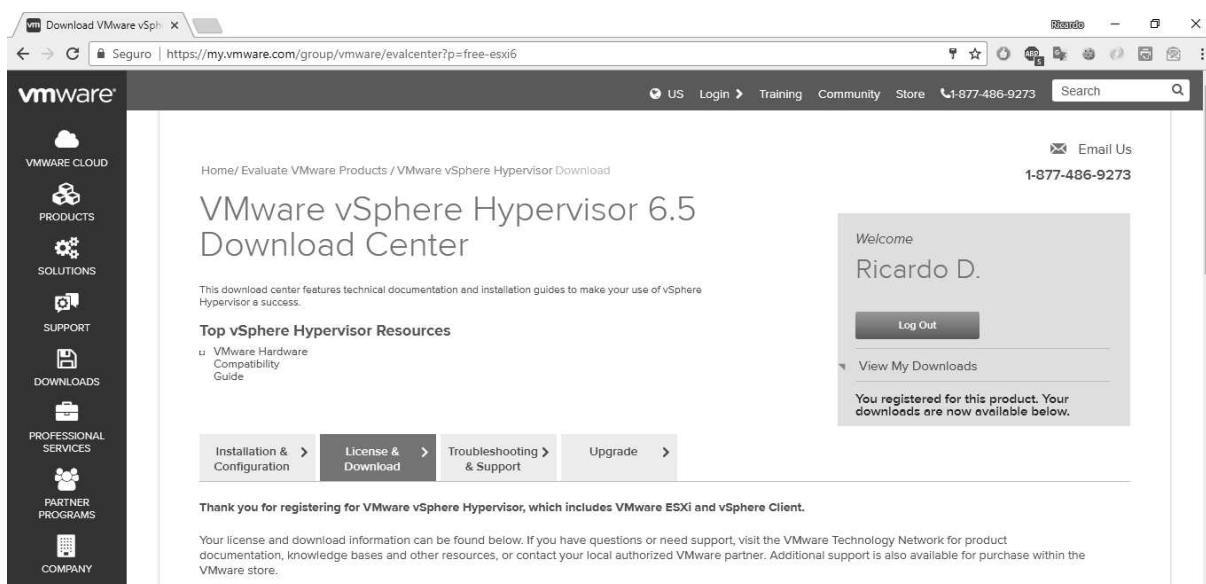


Figura A.5 – Área para download do ESXI

Na tela da Figura A.5 é só rolar a página até a seção **Download Packages**, vai estar aberta a opção mostrando a última versão do ESXI e uma opção **Manually Download** ao lado para fazer o download do arquivo ISO (Figura A.6). Nessa mesma tela em **License information** vai ter sido gerado um código de licença que será usado ativar a versão gratuita do ESXI, caso contrário as funcionalidades do ESXI funcionarão somente por 60 dias.

License Information

COMPONENT	LICENSE KEYS
VMware vSphere Hypervisor 6 License	NN030- XXXXXXXXXXXX

Download Packages

Your downloads are available below

VMware vSphere Hypervisor 6.5.0a - Binaries

ESXi ISO image (Includes VMware Tools)
 2017-02-02 | 6.5.0a | 328.26 MB | iso

Boot your server with this image in order to install or upgrade to ESXi (ESXi requires 64-bit capable servers). This ESXi image includes VMware Tools.

MD5SUM(*): cee025ba50f18d8b06a8025bd1134d5
SHA1SUM(*): fbfe38e102543427d4c62f4033cd292999325e8
SHA256SUM(*): bcbd495b7fd33796b89bbe9ef03fcd31f10a943cc30255353565131b7397a9

Figura A.6 – Última versão do ESXI para download e Licença

Com arquivo ISO da última versão do ESXI baixado, bastará gravar em um CD ou utilizar alguma ferramenta como o Rufus disponível em <https://rufus.akeo.ie/>, para gerar um pendrive bootável com o instalador, e assim seguir para o próximo passo que é fazer a instalação do ESXI no hardware físico.

A.3 INSTALANDO O ESXI 6.5

O processo de início de instalação do ESXI é o mesmo de outros sistemas operacionais, basta colocar o cd/dvd na unidade ou espetar o pendrive bootável em uma porta usb. Depois é necessário configurar no BIOS ou por meio do menu de boot para que o equipamento inicie pelo dispositivo que contém o instalador do ESXI, ao inicializar o dispositivo será carregado módulos e drivers necessários para prosseguir com a instalação como pode ser visto na Figura A.7.



Figura A.7 – Carregamento de módulos da instalação do ESXI

Assim que os módulos e drivers necessários para a instalação estiverem sido carregados, será mostrada a tela da Figura A.8 dando boas-vindas ao processo de instalação. Nessa tela é preciso escolher entre cancelar ou continuar a instalação, teclando **ENTER** para continuar com a instalação, será aberta a tela da Figura A.9 para aceitar os acordos de licenças.

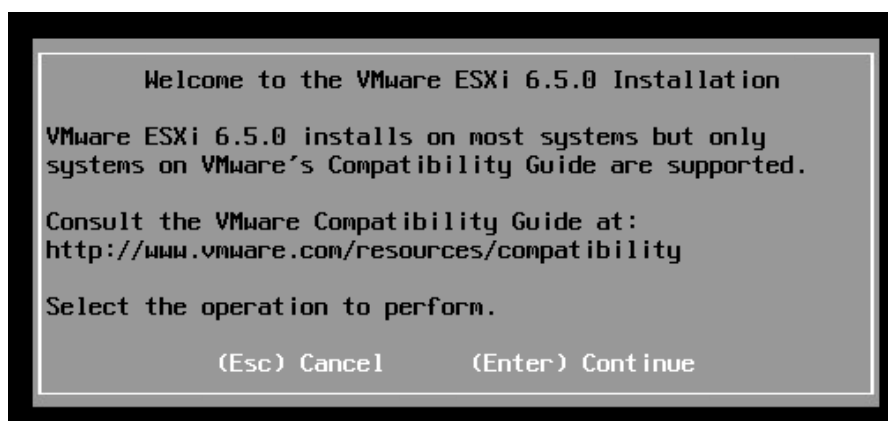


Figura A.8 – Boas-vindas instalação do ESXI

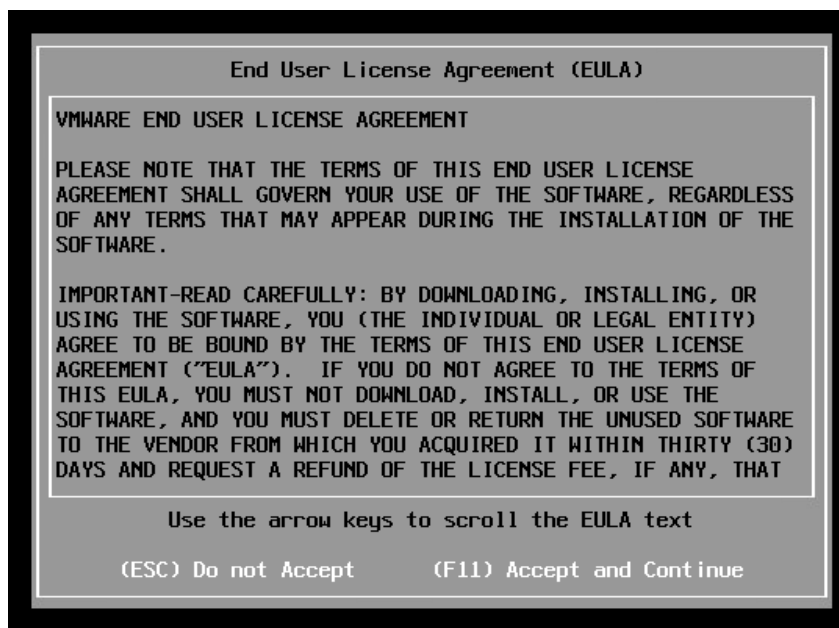


Figura A.9 – Acordo de licença do ESXI

Teclando **F11** na tela da Figura A.9 para aceitar os termos de licenças, o instalador fará uma busca pelos dispositivos de armazenamento disponíveis para a instalação. Com os dispositivos encontrados a tela da Figura A.10 será mostrada, com as setas de direção deverá ser selecionado o dispositivo na qual o ESXI será instalado e em seguida teclar **ENTER** para continuar.

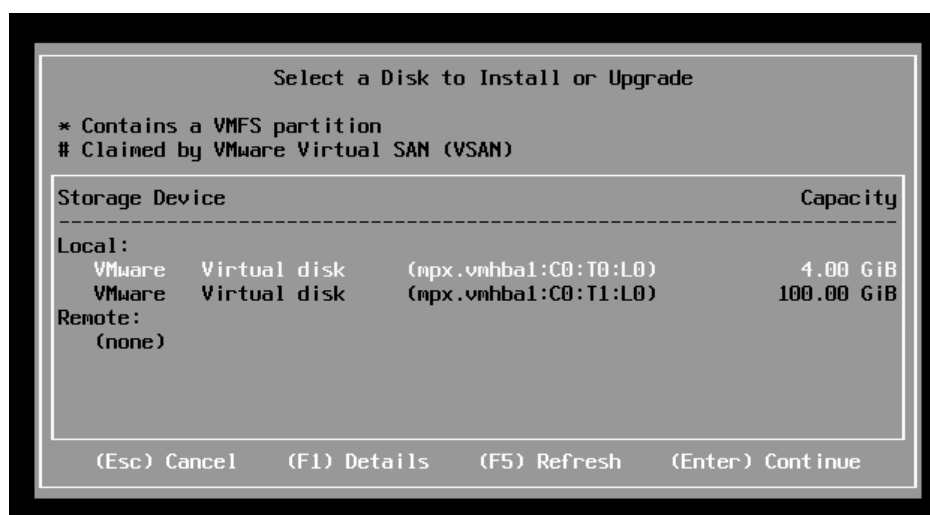


Figura A.10 – Instalação do ESXI dispositivo de armazenamento

Após a escolha do dispositivo de armazenamento que será instalado o ESXI, será aberta uma tela para a escolha do *layout* do teclado (Figura A.11). Com o *layout*

selecionado basta teclar **ENTER** para continuar, será aberta a tela para digitar a senha do usuário *root* (Figura A.12), essa senha será utilizada para acessar a console web de administração e para realizar todas as operações administrativas do ESXI.



Figura A.11 – Instalação do ESXi *layout* do teclado



Figura A.12 – Definição da senha do usuário *root*

Com a senha informada e teclando **ENTER** para continuar, será aberto a tela da Figura A.13 solicitando a confirmação da instalação no dispositivo de armazenamento escolhido e informando que o disco será reparticionado, nessa tela é preciso teclar **F11** para que o processo de instalação seja iniciado. O processo de instalação demorará um pouco e mostrará uma barra com o processo de instalação (Figura A.14).

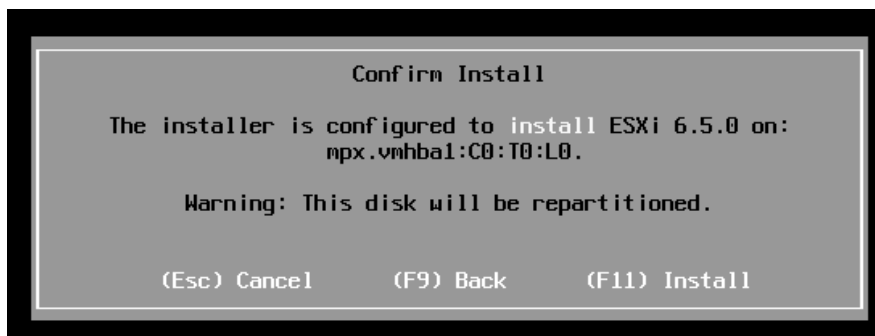


Figura A.13 – Confirmação da instalação do ESXI



Figura A.14 – Progresso da instalação do ESXI

Após o processo de instalação, será mostrada a tela da Figura A.15 informando que a instalação foi completada com sucesso, e que o ESXi irá funcionar com licença de avaliação por 60 dias sendo necessário após esse período utilizar uma licença. Além disso, é informado que para administrar o ESXi deve-se utilizar o IP em um navegador, também solicita que seja removido o dispositivo utilizado para instalação e que é preciso teclar **ENTER** para reiniciar o sistema.



Figura A.15 – Instalação do ESXI completada

Depois que o sistema reiniciar a tela da Figura A.16 será aberta. Nessa tela é mostrado algumas informações do *hardware* utilizado, como memória e processador. Essa tela também mostra o IP que foi obtido automaticamente por meio do DHCP, é esse IP que será utilizado para acessar a administração do ESXI utilizando um navegador web.

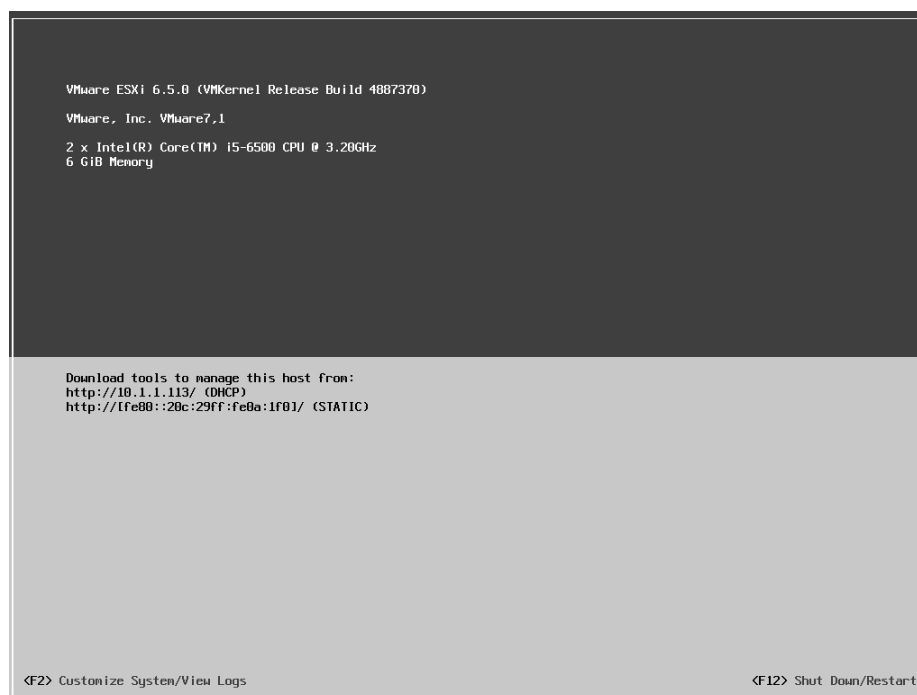


Figura A.16 – Tela depois do carregamento do ESXI

Ainda na tela da Figura A.16 é possível fazer bem poucas configurações. Teclando **F2** nessa tela será solicitada a senha de *root* e em seguida abrirá a tela da Figura A.17. Nessa tela é possível redefinir a senha, configurar, reiniciar, testar e restaurar a interface de rede de gerenciamento, configurar *layout* do teclado, configurar opções para resolução de problemas, visualizar *logs* e redefinir as configurações de sistema.

Como pode ser visto, diretamente no ESXI não é possível fazer muita coisa no que se refere ao ambiente virtualizado, pois todas as operações com máquinas virtuais são feitas utilizando a web UI que é um ambiente de administração web do ESXI.

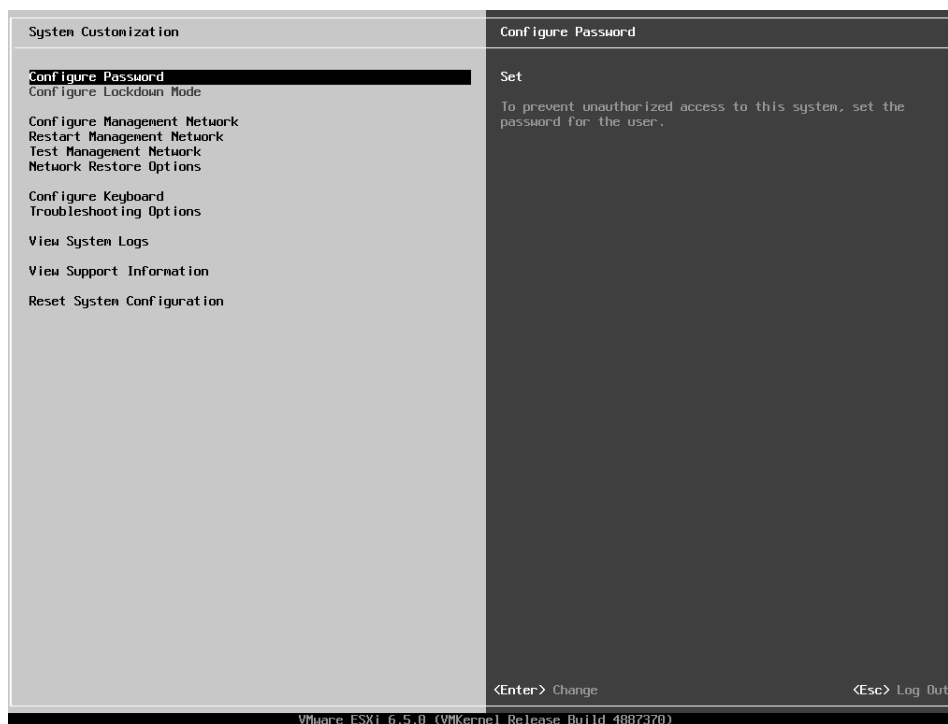


Figura A.17 – Configurações do ESXI pelo console

A.4 ACESSANDO O AMBIENTE DE ADMINISTRAÇÃO DO ESXI

Para acessar o ambiente de administração do ESXI, é preciso abrir um navegador web e informar o IP configurado no ESXI, será aberto a página da Figura A.18 solicitando o usuário e senha para ter acesso ao ambiente, o usuário é *root* e a senha a que foi cadastrada no processo de instalação. Informando o usuário e senha e clicando em **Log in** será aberto o *dashboard* do ambiente de administração (Figura A.19).

Todas as operações no ambiente virtualizado será realizada nessa tela, o menu do lado esquerdo da tela está dividido em dois grupos. Um dos grupos onde está o *host* ESXI é utilizado para monitorar o ambiente e fazer configurações do próprio *host* do ESXI, como habilitar serviços, configurar servidor NTP, configurações de segurança, licença, configurações avançadas entre outras. No outro grupo estão as opções para gerenciar as VMs, dispositivos de armazenamento e rede do ambiente.

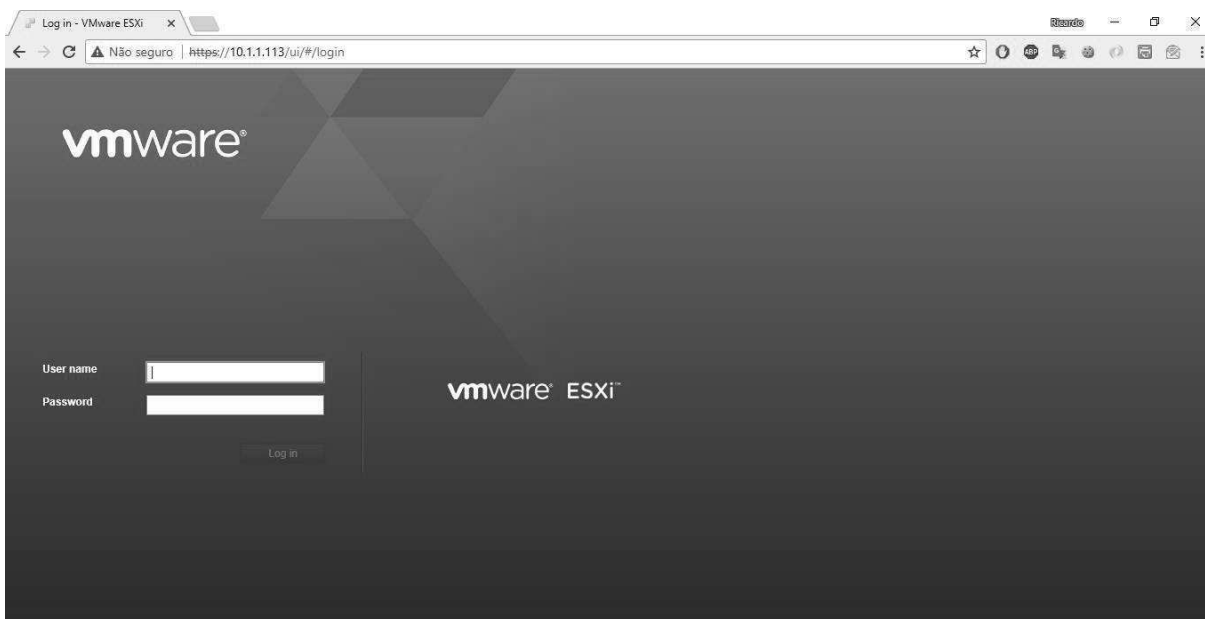


Figura A.18 – Tela de login do ambiente de administração do ESXI

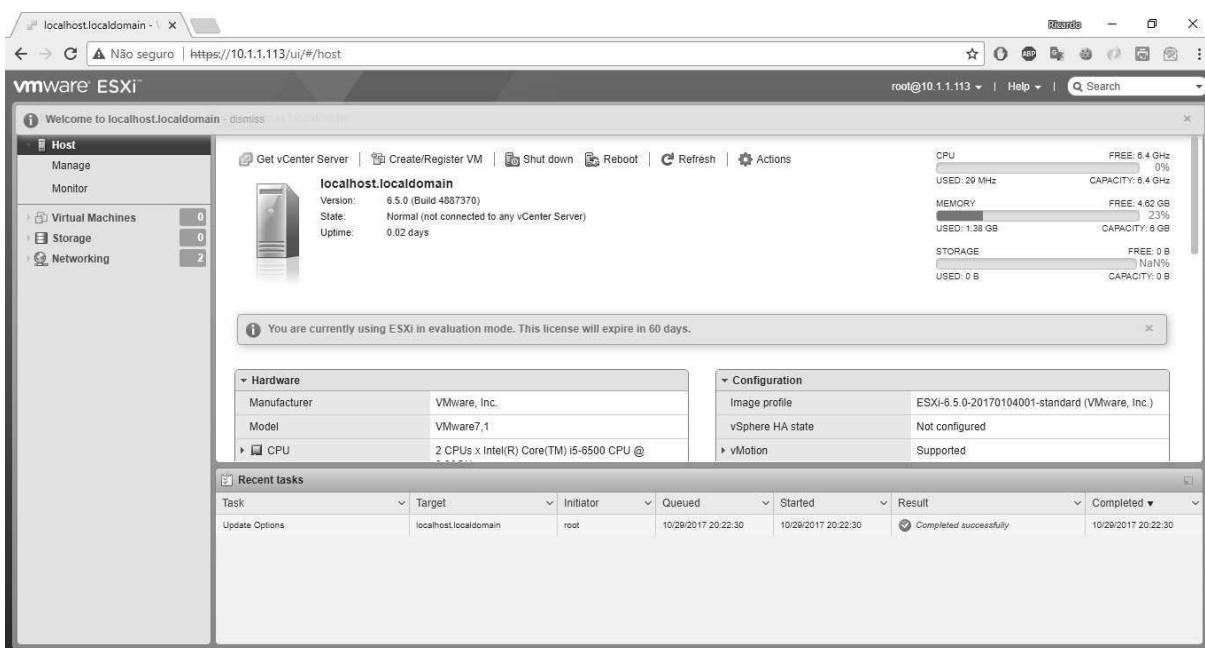


Figura A.19 – Dashboard de administração do ESXI

A.5 ADICIONANDO A LICENÇA GRATUITA DO ESXI

Quando foi feito o download do ESXI no site da VMWare, foi gerada uma licença para utilização do ESXI gratuitamente com algumas limitações. Para

adicionar essa licença ao ESXI instalado é preciso clicar em **Manage** no menu esquerdo do ambiente de administração, e depois em **Licensing**, e em seguida clicar em **Assign license** (Figura A.20). Na próxima tela que abrir basta digitar o código de licença no campo correspondente e clicar em **Check license** (Figura A.21).



Figura A.20 – Tela para adicionar a licença gratuita do ESXI

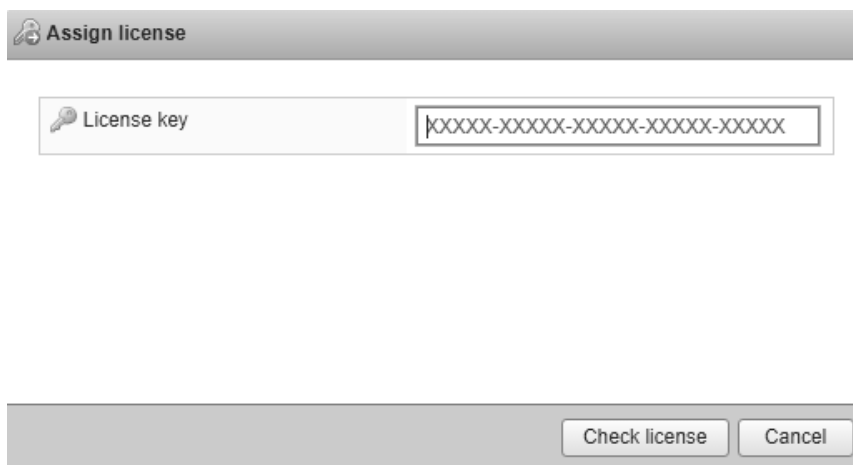


Figura A.21 – Tela para adicionar a licença gratuita do ESXI

Se a licença informada for válida será mostrada a tela da Figura A.22, agora é só clicar em **Assign licence** para associar a licença ao ESXI instalado. Com a licença associada ao ambiente, o *dashboard* já mostrará os recursos que estarão disponíveis para essa licença (Figura A.23).

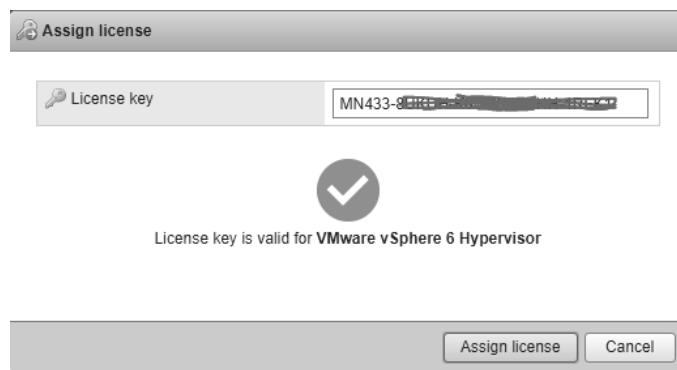


Figura A.22 – Tela para adicionar a licença gratuita do ESXI

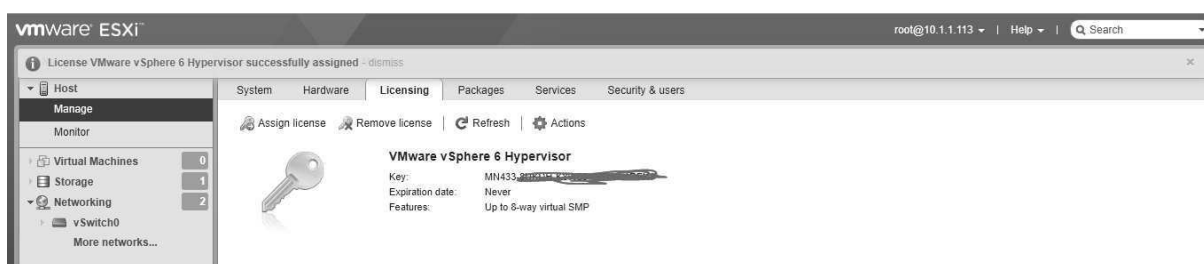


Figura A.23 – ESXI ativado com a licença gratuita

A.6 CONFIGURANDO DISPOSITIVOS DE ARMAZENAMENTO

No ambiente virtualizado do ESXI o sistema trabalha com o conceito de *datastore* que é uma abstração dos dispositivos de armazenamento. O *datastore* é formatado com um sistema de arquivos chamado VMFS (*Virtual Machine File System*) otimizado para armazenamento de arquivos de máquinas virtuais. Depois de instalado o ESXI é necessário criar esses *datastores* no ambiente para poder armazenar os arquivos das VMs.

Estando logado no ambiente de administração do ESXI, é preciso clicar em **Storage** e depois em **New datastore** no menu esquerdo do ambiente (Figura A.24).

Depois de clicar nessas opções será aberto a tela da Figura A.25, que permitirá selecionar se o objetivo é criar um novo *datastore*, aumentar o tamanho de um já existente ou montar um *datastore* utilizando um armazenamento do tipo NFS.

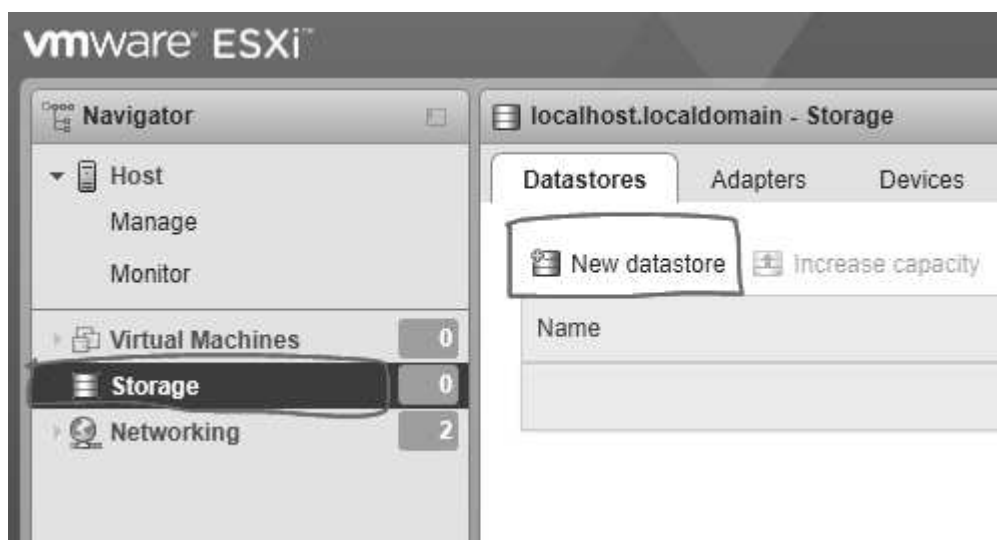


Figura A.24 – Opção New *datastore* ESXI

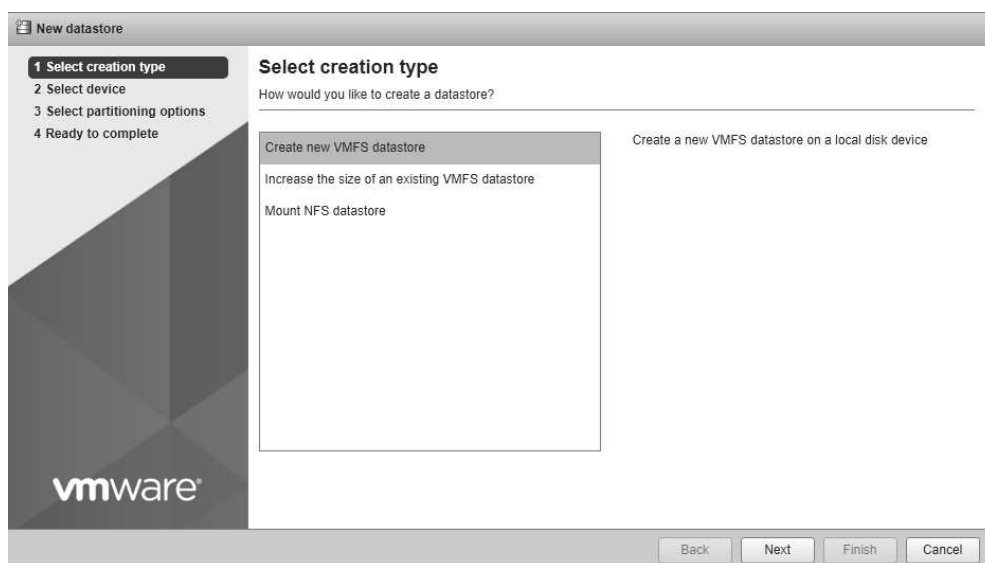


Figura A.25 – Criação de *datastore* no ESXI

Selecionando a opção **Create new VMFS datastore** na tela da Figura A.25 e clicando em **Next**, será aberto a tela da Figura A.26, essa tela mostra os dispositivos de armazenamento detectados pelo ESXI para que seja selecionado um deles, além disso é preciso informar um nome para o novo *datastore* que será criado.

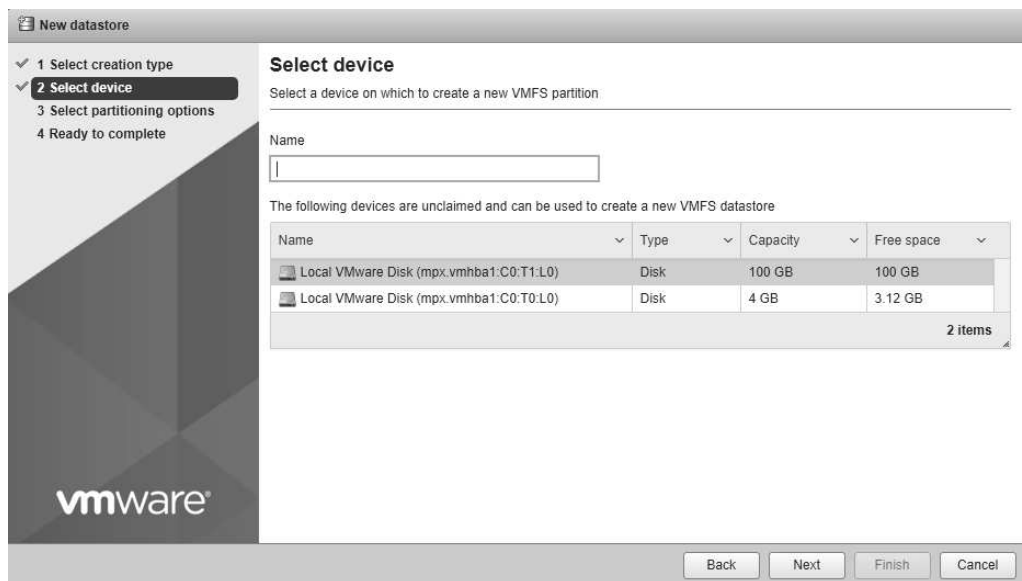


Figura A.26 – Nome do *datastore* e seleção do dispositivo

Após informar o nome do *datastore* e selecionar um dispositivo de armazenamento, ao clicar em **Next** a tela da Figura A.27 será mostrada. Nessa tela é possível escolher a versão do VMFS e também informar se será utilizado todo o espaço disponível no dispositivo ou somente parte dele para a criação do *datastore*.



Figura A.27 – Tamanho da partição e versão do VMFS

Feito as configurações de tamanho de partição e versão do VMFS e clicando em **Next**, será aberta a tela da Figura A.28, que mostra um resumo de todas as opções escolhidas anteriormente, clicando em **Finish** o processo de criação do

datastore é finalizado, uma mensagem dizendo que todos os dados do dispositivo serão perdidos é mostrada, é só clicar em **Yes** para aceitar.

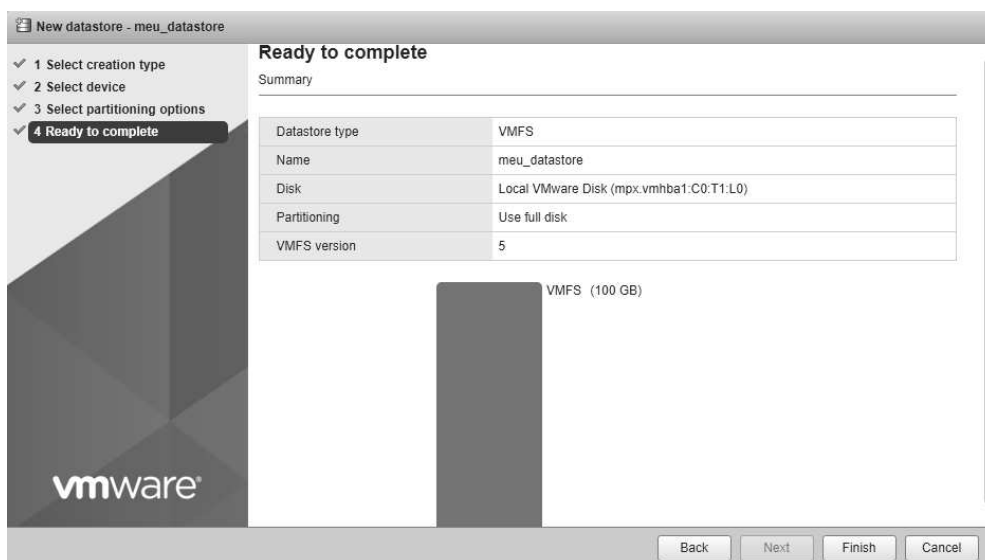


Figura A.28 – Resumo das configurações do *datastore* a ser criado

Depois de criado o *datastore*, no *dashboard* do ESXI em **Storage**, já será possível ver e utilizar o novo *datastore* (Figura A.29). Clicando na opção **Datastore browser** é possível navegar pelo conteúdo do *datastore*, criar pasta, enviar, excluir, mover, copiar e fazer download de arquivos (Figura A.30).

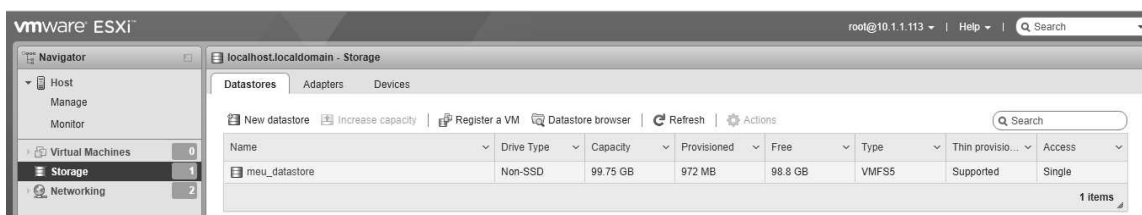


Figura A.29 – *Datastore* recém-criado no ESXI



Figura A.30 – *Datastore browser* no ESXI

A.7 CONFIGURANDO A REDE NO AMBIENTE VIRTUALIZADO

Para conseguir utilizar as interfaces físicas no ESXI é preciso associá-la a um *virtual switch* e esse por sua vez deve ser associado a um *port group*. O vSwitch funciona como um *switch* físico, possui portas onde serão conectadas as VMs e a conexão com a interface física é chamada de *uplink*, que é a saída para a rede física. O *port group* funciona somente como um agrupamento, no momento de configurar a VM em vez de associar a interface virtual a uma porta no vSwitch, a interface é associada a um *port group* e assim já estará conectada ao vSwitch na qual o *port group* está associado.

No processo de instalação do ESXI é criado automaticamente o vSwitch0 e feito o *uplink* com a interface física primária, também são criados os *ports group* **VM Network** e **Management Network** (Figura A.31). As outras interfaces não estão associadas a nenhum vSwitch e não podem ser utilizadas enquanto isso não for feito, a seguir será mostrado como criar um vSwitch associar a uma interface de rede e criar um *port group* e associar ao vSwitch.

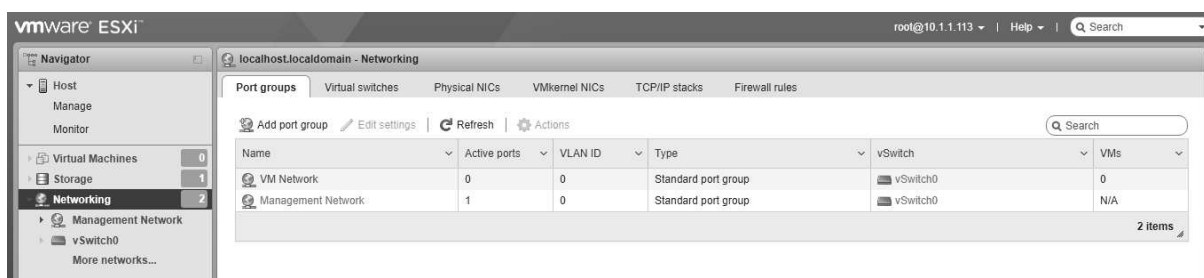


Figura A.31 – vSwitch e *ports group* criados na instalação do ESXI

Para criar um vSwitch é preciso acessar **Networking** no menu esquerdo do *dashboard* em seguida clicar em **Virtual Switch** e depois em **Add standard virtual switch** (Figura A.32). Será aberto a tela da Figura A.33, nessa tela é preciso informar o nome do vSwitch a ser criado e qual interface de rede será o *uplink*. Ao clicar em **Add** o vSwitch será criado e já estará disponível no ambiente do ESXI (Figura A.34).

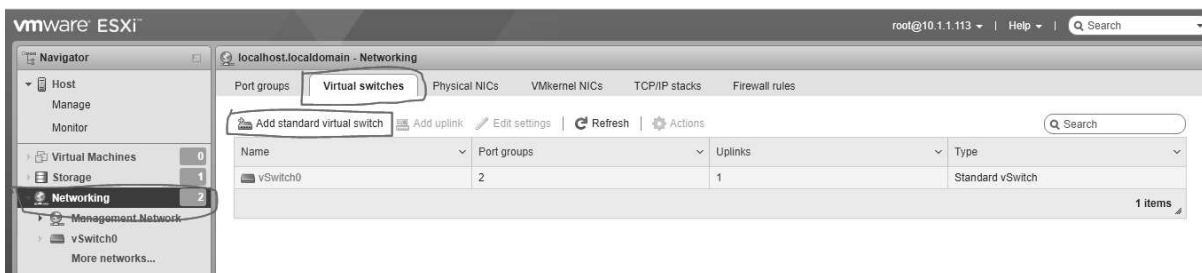


Figura A.32 – Opção para adicionar um vSwitch no ESXi

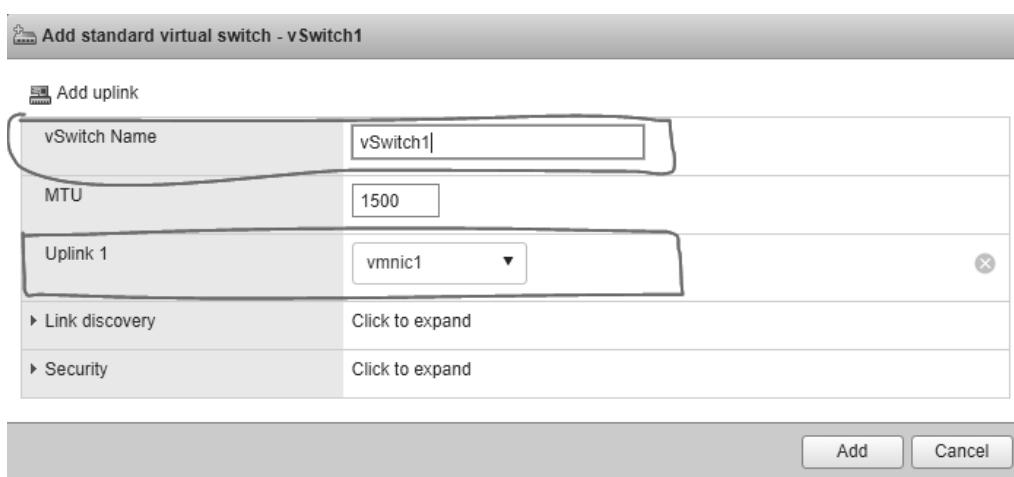


Figura A.33 – Tela para criação do vSwitch

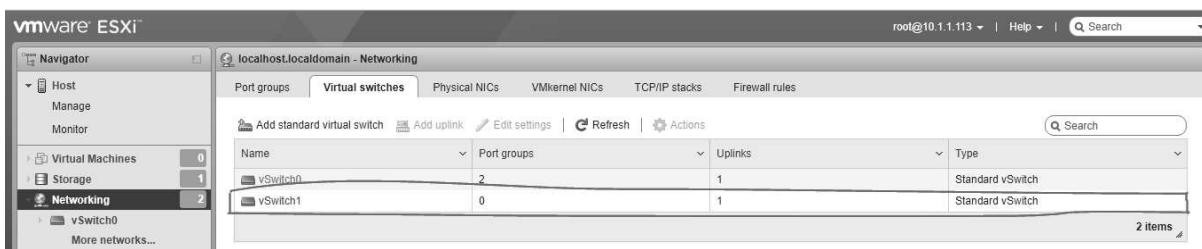


Figura A.34 – Tela para criação do vSwitch

Com o vSwitch1 criado, falta criar um *port group* e associa-lo a ele. Para criar o *port group* é preciso clicar em **Networking** depois em **Port Group** e em **Add port group**, a tela da Figura A.35 será exibida. Nessa tela deve ser informado o nome do *port group* e selecionar o *virtual switch* que ele estará associado e clicar em **Add**, depois desses passos o *port group* já estará criado (Figura A.36).

Add port group - VM Network 1

Name	VM Network 1
VLAN ID	0
Virtual switch	vSwitch1
Security	Click to expand

Buttons: Add, Cancel

Figura A.35 – Tela para criação do *Port Group*

Name	Active ports	VLAN ID	Type	vSwitch	VMs
VM Network	0	0	Standard port group	vSwitch0	0
Management Network	1	0	Standard port group	vSwitch0	N/A
VM Network 1	0	0	Standard port group	vSwitch1	N/A

Figura A.36 – *Port group* VM Network 1 criado no ambiente

A.8 HABILITANDO O NTP NO ESXI

Em um ambiente virtualizado da VMWare as máquinas virtuais sincronizam a hora diretamente com o *host* físico. Se o horário do *host* estiver errado vários problemas podem ser gerados nos serviços executados pelas VMs, controladores de domínio terão problemas de sincronização, servidores de arquivos com *timestamp* incorretos, banco de dados com entradas incorretas, além disso os *logs* do ambiente são ótimas ferramentas de auditoria, mas nesse caso não poderão ser utilizados.

O ESXI suporta o protocolo NTP (*Network Time Protocol*) que permite a sincronização de tempo com relógios atômicos e sistema GPS. Esse protocolo utiliza uma estrutura em árvore que permite ele trabalhar como cliente e servidor ao mesmo tempo. Existem muitos servidores NTP disponíveis na internet mantidos por órgãos confiáveis, por isso sua exatidão é muito grande, geralmente os desvios de horários são de apenas alguns milissegundos.

Para configurar o NTP no ESXI, primeiramente é preciso verificar se a porta UDP 123 está liberada para conexões de saída, caso o ambiente possua um *firewall* ativo. O próximo passo é acessar o ambiente de administração e clicar em **Manage** e depois em **System** e em seguida em **Time & Date** (Figura A.37).

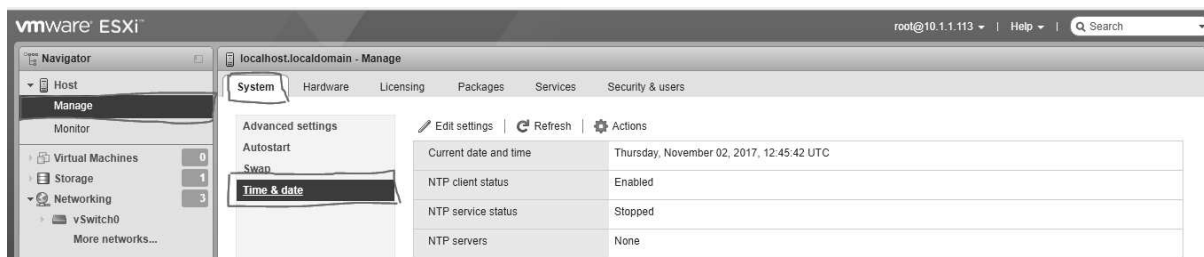


Figura A.37 – Configuração do NTP no ESXI

Na tela da Figura A.37 provavelmente o NTP estará parado, para configurá-lo e iniciá-lo, é só clicar em **Edit Settings**, a tela da Figura A.38 será aberta. Nessa tela deve ser selecionada a opção **Use Network Time Protocol (enable NTP client)**, e depois escolher em **NTP service startup policy** a política de início do serviço, que nesse caso foi selecionado para iniciar e parar com o *host*, além disso é preciso em **NTP Servers** informar o servidor ou servidores NTP na qual o *host* será sincronizado, aqui foi colocado um único servidor *pool.ntp.br* que é composto por vários outros servidores.

Feita essas configurações e clicando em **Save**, as configurações serão salvas, e a próxima vez que o *host* for iniciado o serviço também será iniciado. Com isso o *host* ESXI já estará configurado para sincronizar seu horário com servidores NTP na internet, e as VMs sincronizarão seus horários com o *host*.

Figura A.38 – Configurações do NTP

A.9 COMO CRIAR E CONFIGURAR UMA MÁQUINA VIRTUAL NO ESXI

Depois de realizar as configurações anteriores, o ambiente já estará pronto para a criação das máquinas virtuais, nesse capítulo será mostrada a criação e configuração de uma máquina virtual, e para a criação de outras VMs os passos são semelhantes, bastando alterar algumas configurações. Acessando o ambiente de administração do ESXI e clicando em **Virtual Machines** nenhuma máquina virtual será mostrada (Figura A.39), para iniciar a criação da VM é só clicar em **Create / Register VM**, a tela da Figura A.40 será exibida.

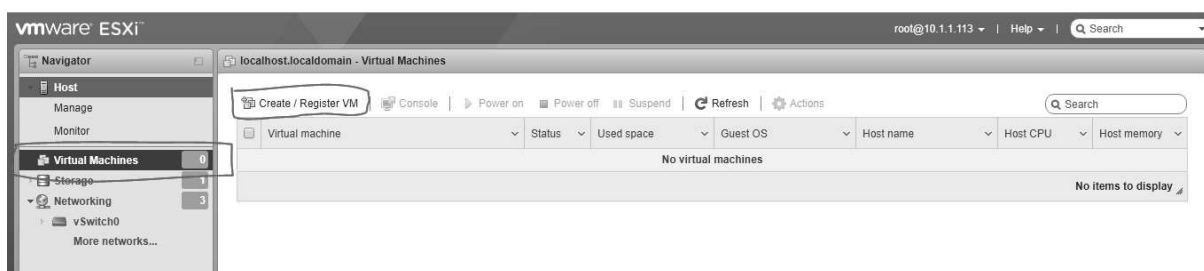


Figura A.39 – Criação da máquina virtual

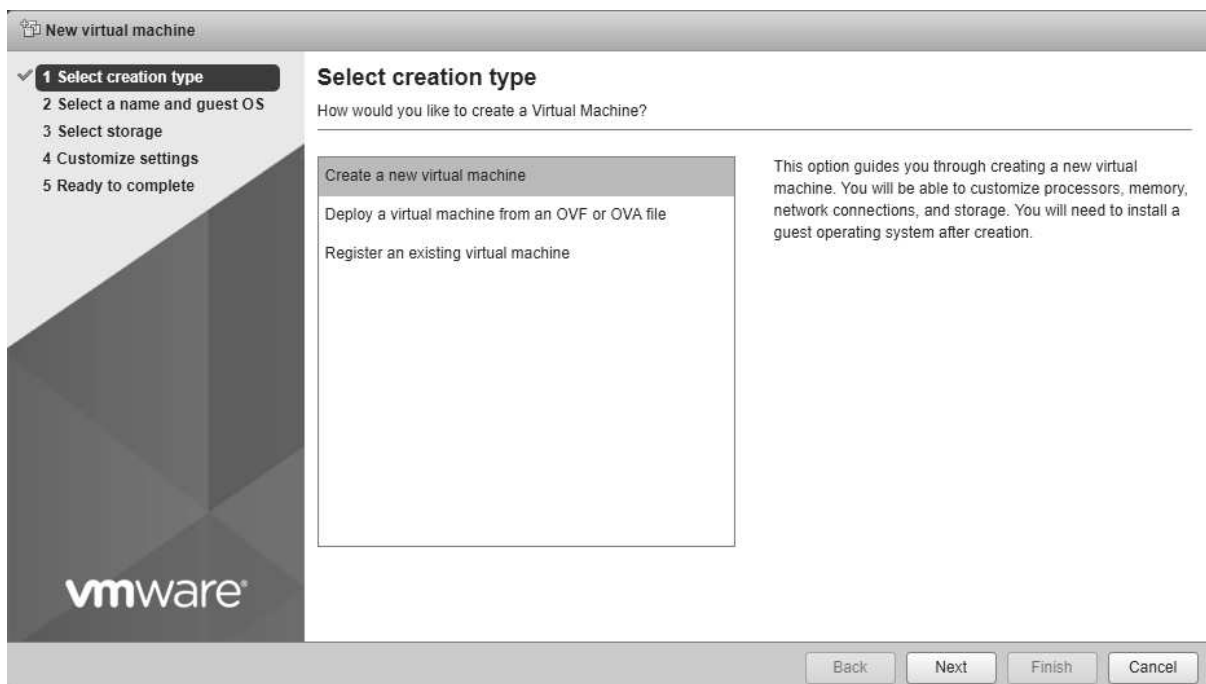


Figura A.40 – Passo a passo para configuração da VM

Na tela da Figura A.40 deve ser selecionado umas das três opções: **Create a new virtual machine** para a criação de uma máquina virtual a partir do zero, **Deploy a virtual machine from an OVF or OVA file** permite restaurar uma VM que tenha sido exportada e salva em um arquivo OVF ou OVA, **Register an existing virtual machine** caso a máquina virtual já exista em um *datastore* no *host*, essa opção é usada para registra-la no ambiente do ESXI.

Selecionando a opção para criação de uma nova máquina virtual e clicando em **Next** a tela da Figura A.41 será aberta. Nessa tela é necessário informar o nome da máquina virtual, em **Compatibility** deve ser selecionado a versão do ESXI que a máquina virtual será compatível, em **Guest OS Family** é preciso selecionar a família do SO convidado, e em **Guest OS version** a versão do SO, depois clicando **Next** a tela da Figura A.42 será aberta.

Essa tela mostrará os *datastores* disponíveis no ambiente no ESXI, é preciso selecionar um deles onde será armazenada a máquina virtual, nesse ambiente somente um *datastore* está disponível então basta clicar em **Next** para prosseguir.

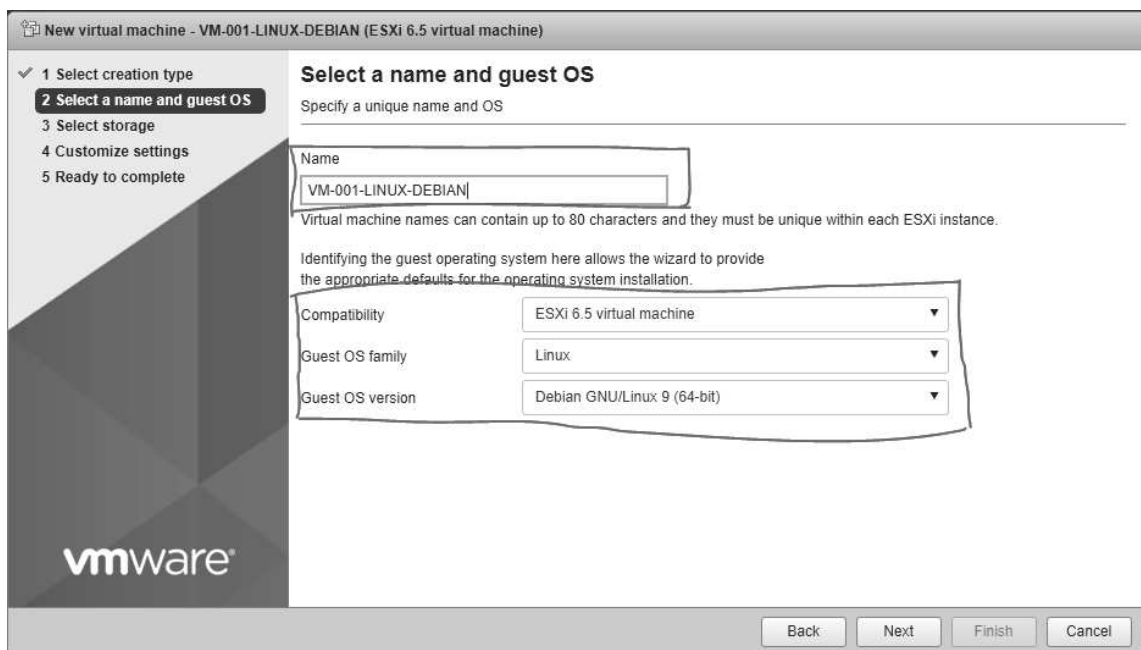


Figura A.41 – Nome da VM, SO convidado e compatibilidade



Figura A.42 – Datastores para armazenamento das VMs

Depois de selecionado o *datastore* a próxima tela aberta é a da Figura A.43, nessa tela é onde deve ser feita as configurações de *hardware* da VM como, CPU, memória, disco, interface de rede etc. Em **CPU** é listado cada núcleo do processador físico como um processador virtual, aqui deve ser selecionado a quantidade de

núcleos que a VM terá disponível para ela. Em **memory** deve ser informada a quantidade de memória que a VM terá.



Figura A.43 – Configurações de hardware da VM

Clicando em **Hard disk 1** a tela da Figura A.44 será aberta, é nessa tela que será definido o tamanho do disco da VM. Além disso, é possível também mudar o local onde o disco virtual será armazenado.

Em **Drive Provisioning** existe três opções importantes, **Thin provisioned** irá criar o disco, mas não ocupará todo o tamanho informado, e conforme a demanda ele irá ocupar mais espaço até o limite informado, **Thick provisioned, lazily zeroed** criará o disco com o tamanho especificado e não sobrescreverá o conteúdo que já existia no disco, **Thick provisioned, eagerly zeroed** cria o disco com o tamanho especificado, e além disso sobrescreverá todo o conteúdo existente com zeros.

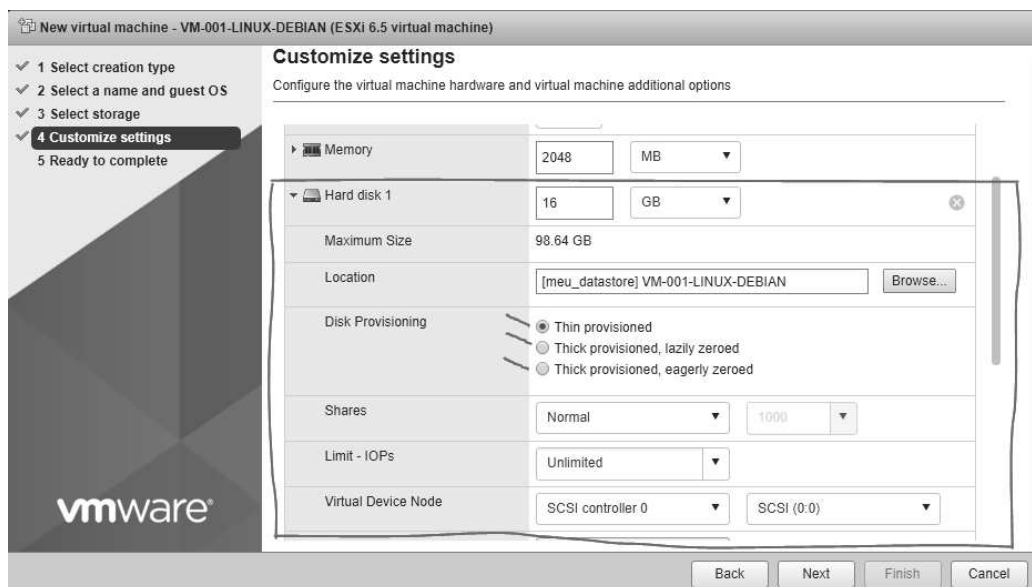


Figura A.44 – Configurações de disco da VM

Por padrão uma interface de rede virtual é adicionada na VM, e essa interface é vinculada ao primeiro *port group*, que nesse caso é o **VM Network** (Figura A.45), mas é possível mudar para um outro *port group* bastando clicar na caixa de seleção. Também é possível adicionar mais interfaces de redes clicando em **Add network adapter**, a interface será adicionada e poderá ser selecionado em qual *port group* ela estará vinculada.

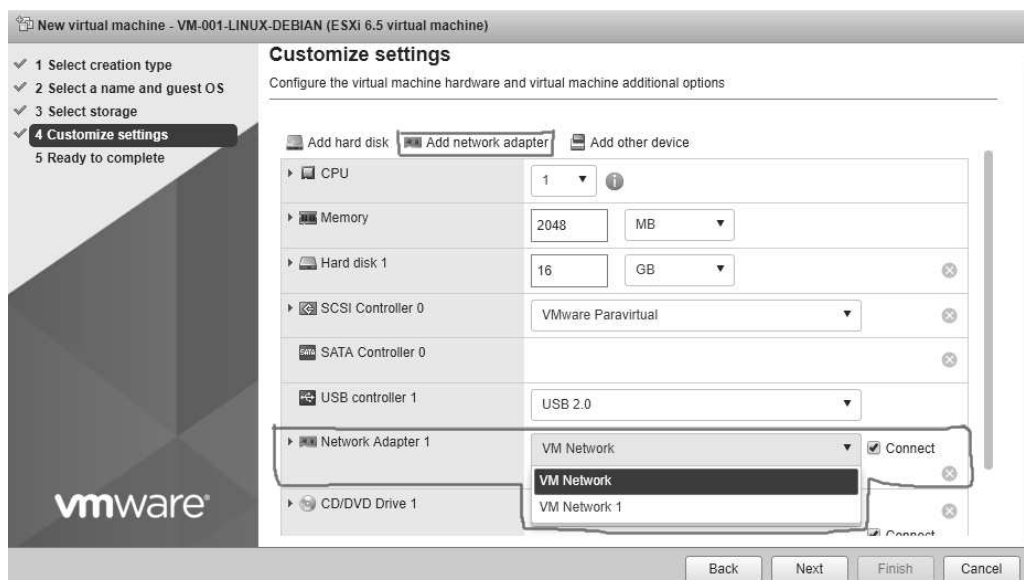


Figura A.45 – Configurações de rede da VM

Outro dispositivo de *hardware* virtual que é adicionado na VM por padrão é o **CD/DVD Drive**, esse dispositivo é usado para montar um arquivo ISO do instalador do sistema operacional que será instalado na VM (Figura A.46). Para usar um arquivo ISO é preciso selecionar **Datastore ISO file** na caixa de seleção e depois no campo **CD/DVD Media** selecionar o arquivo ISO do instalador, lembrando que o arquivo deve estar dentro de um *datastore* do *host*.

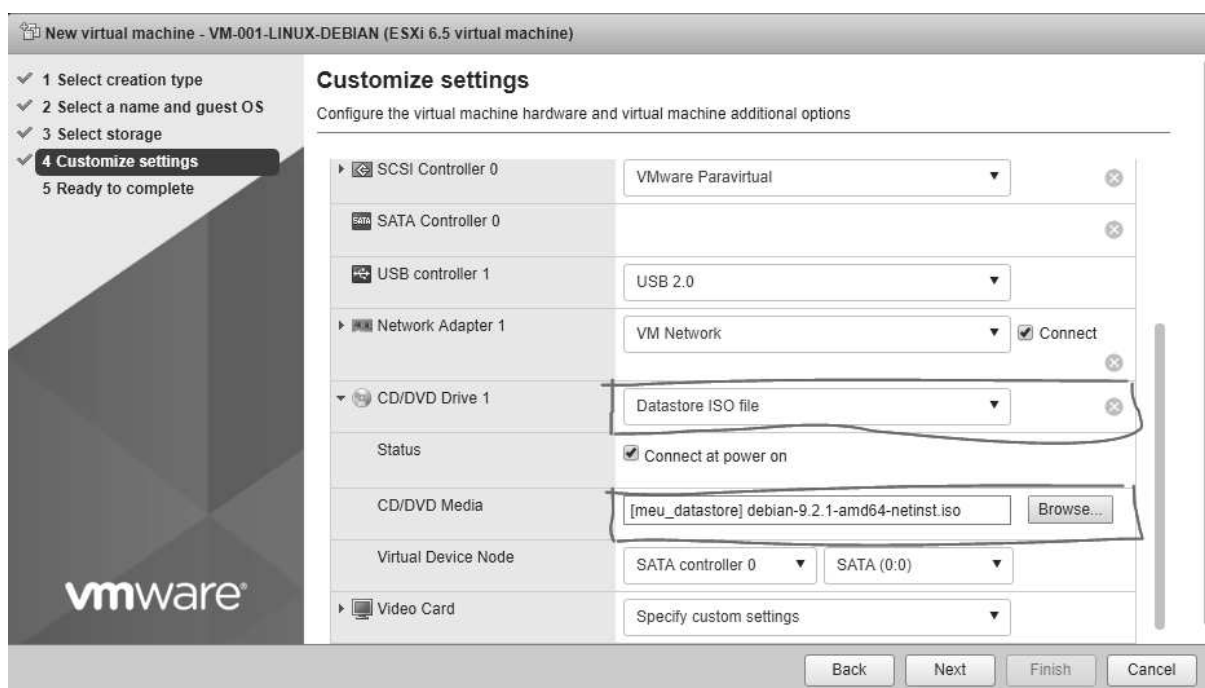


Figura A.46 – Configurações de rede da VM

Voltando para o topo da tela de configurações de *hardware*, e clicando em **VM Options** e depois em **VMware Tools** (Figura A.47), rolando essa tela até achar as opções destacadas na Figura A.48, essas opções devem ser marcadas. A primeira opção **Check and upgrade VMware Tools before each power on** irá manter o pacote vmware tools atualizados no SO convidado, a outra opção **Synchronize guest time with host** sincronizará o horário do SO convidado com o host ESXI.

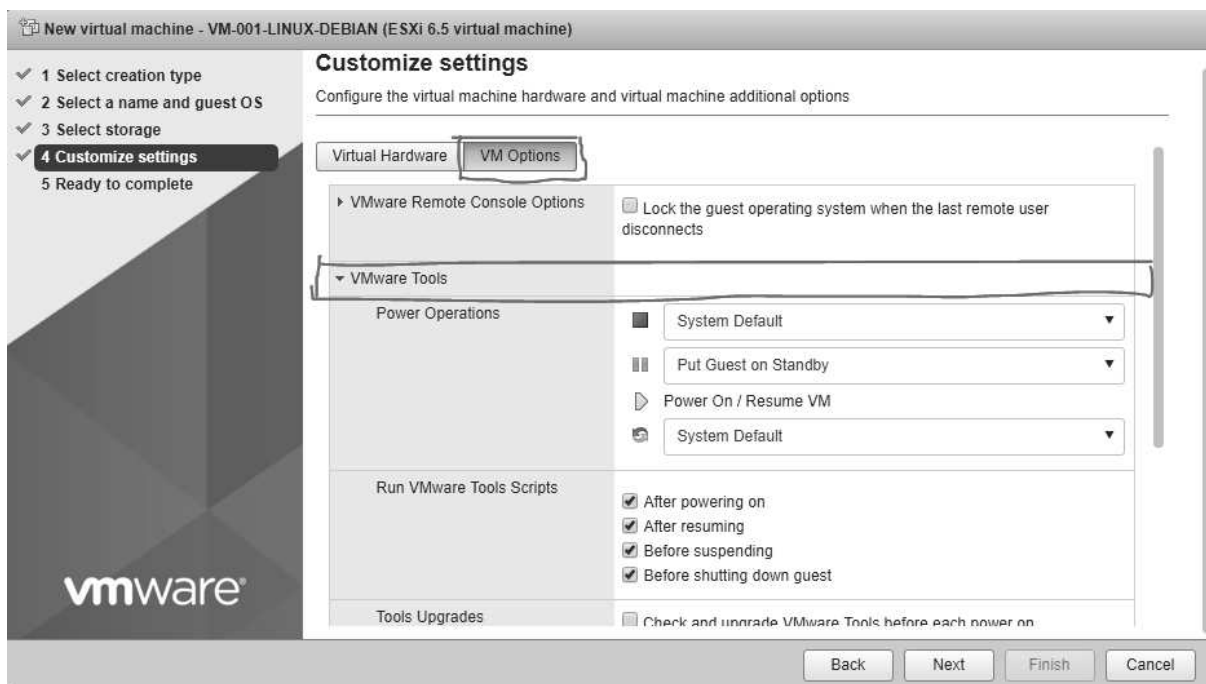


Figura A.47 – VM Options

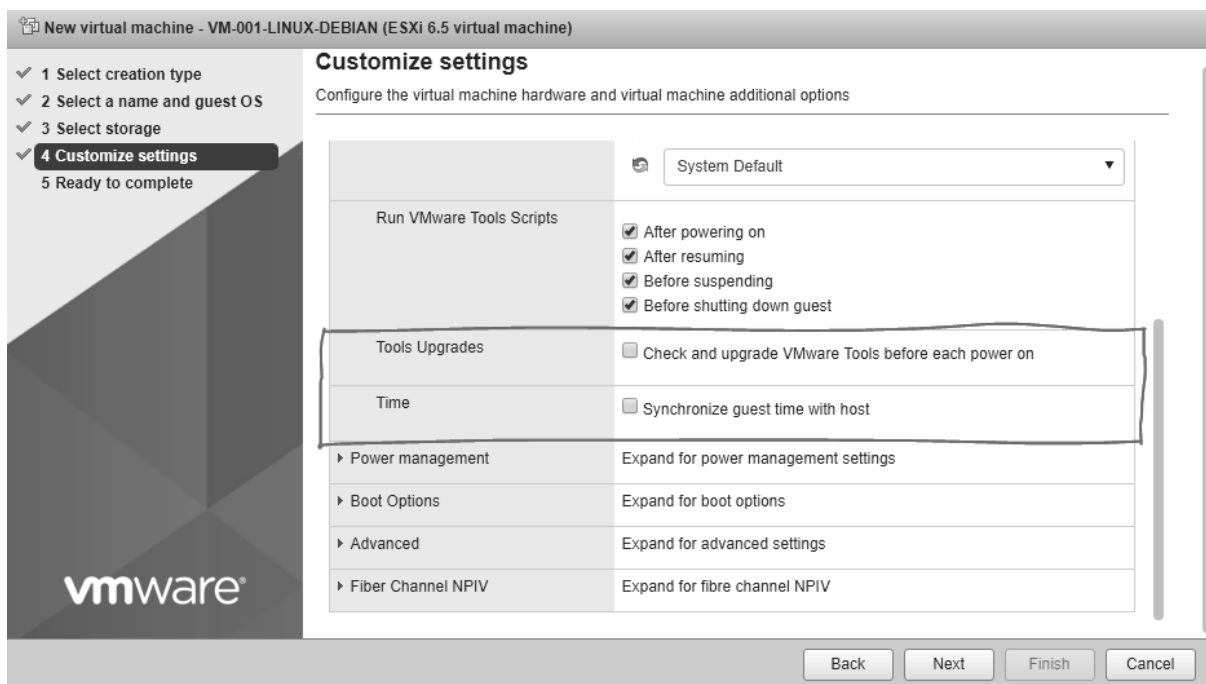


Figura A.48 – VM Options, Tools Upgrades, Time

Com essas configurações realizadas bastará clicar em **Next**, será aberta a tela da Figura A.49 com um resumo de todas as configurações realizadas na VM, caso todas as configurações estejam de acordo, é só clicar em **Finish** para finalizar a criação da VM.

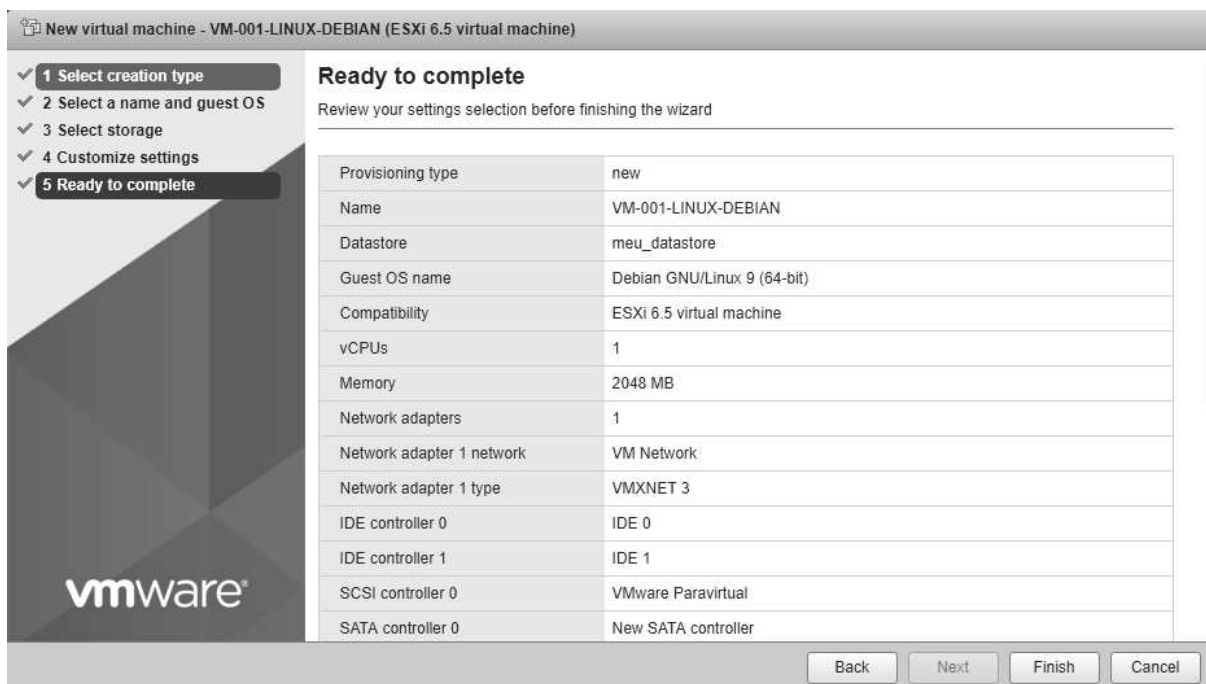


Figura A.49 – Resumo das configurações da VM

Durante as configurações da VM foi selecionado o arquivo ISO de instalação do SO convidado, então depois que a VM for criada, bastará ligá-la clicando na região destacada na Figura A.50 que a máquina virtual será ligada e abrirá uma janela exibindo o SO convidado, essa tela permitirá realizar todas as operações no SO que está sendo instalado (Figura A.51).

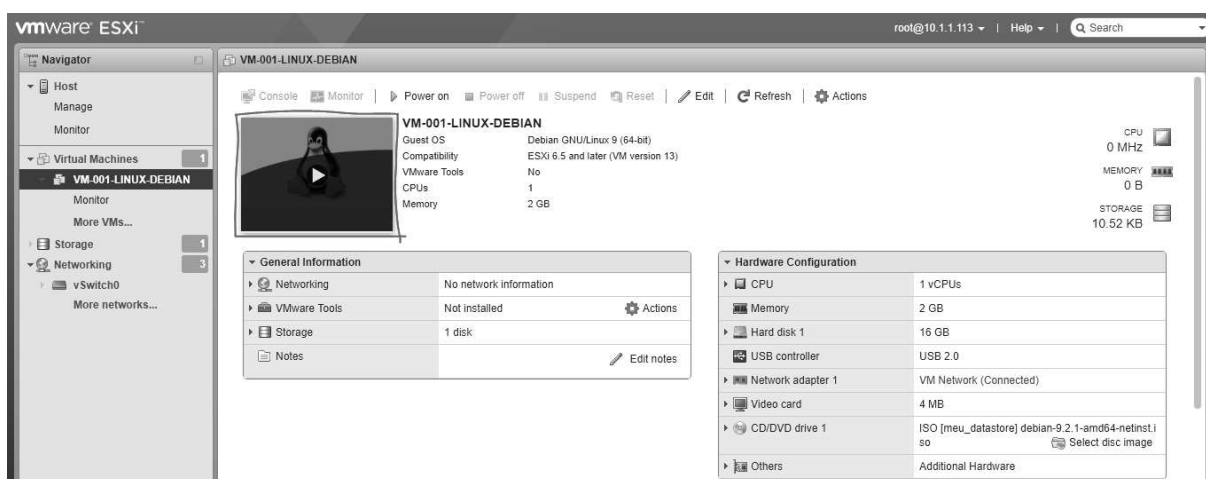


Figura A.50 – Ligando a VM



Figura A.51 – Máquina virtual ligada

A.10 CONSIDERAÇÕES SOBRE A CONFIGURAÇÃO DO ESXI

Os processos de instalação do ESXI mostrados nesse APÊNDICE seguiram os passos padrões do ESXI 6.5, dependendo do *hardware* utilizado e a versão do ESXI as opções poderão ser diferentes das apresentas aqui. As configurações das VMs também poderão mudar dependendo da versão do ESXI e do *hardware* utilizado.

O ESXI possui muitas outras configurações além dessas apresentas nesse APÊNDICE, foi utilizada as configurações principais para que o ambiente esteja funcional. O uso dessas configurações dependerá do ambiente que se está configurando e também do conjunto de hardware utilizado.

Uma recomendação é sempre consultar os documentos disponíveis no site da VMWare e da comunidade VMWare, eles fornecerão uma ótima fonte de pesquisa para conhecimento do ambiente virtualizado, assim como informações sobre configurações avançadas de otimizações que podem ser feitas no ambiente.