



UNIVERSIDADE DE CAXIAS DO SUL
CENTRO DE CIÊNCIAS EXATAS E DA TECNOLOGIA
CIÊNCIA DA COMPUTAÇÃO

BRUNO EMER

Implementação de alta
disponibilidade em uma empresa
prestadora de serviços para Internet

André Luis Martinotto
Orientador

Caxias do Sul
Maio de 2016

Implementação de alta disponibilidade em uma empresa prestadora de serviços para Internet

por

Bruno Emer

Projeto de Diplomação submetido ao curso de Bacharelado em Ciência da Computação do Centro de Ciências Exatas e da Tecnologia da Universidade de Caxias do Sul, como requisito obrigatório para graduação.

Projeto de Diplomação

Orientador: André Luis Martinotto

Banca examinadora:

Maria de Fatima Webber do Prado Lima

CCTI/UCS

Ricardo Vargas Dorneles

CCTI/UCS

Projeto de Diplomação apresentado em
x de julho de 2016

Daniel Luís Notari
Coordenador

SUMÁRIO

LISTA DE SIGLAS	3
LISTA DE FIGURAS	4
LISTA DE TABELAS	5
RESUMO	6
1 INTRODUÇÃO	7
1.1 Objetivos	8
1.2 Estrutura do trabalho	8
2 ALTA DISPONIBILIDADE	9
2.1 Tolerância a falhas	9
2.2 Redundância	11
2.3 Cálculo da alta disponibilidade	12
2.4 Considerações finais	13
3 VIRTUALIZAÇÃO	14
3.1 Máquinas virtuais de aplicação	16
3.2 Máquinas virtuais de sistema	17
3.2.1 Arquiteturas de máquinas virtuais de sistema	17
3.2.2 Implementações de máquinas virtuais de sistema	18
3.3 Vantagens das máquinas virtuais	20
3.3.1 Virtualização de Desktop	20
3.3.2 Virtualização de servidores	20
3.4 Considerações finais	21
4 ESTUDO DE CASO	22
4.1 Ambiente físico e virtual	22
4.2 Serviços críticos	31
5 PROPOSTA DE SOLUÇÃO	33
REFERÊNCIAS	34

LISTA DE SIGLAS

ADSL	<i>Asymmetric Digital Subscriber Line</i>
API	<i>Application programming interface</i>
ASP	<i>Active server pages</i>
DNS	<i>Domain name system</i>
ECC	<i>Error correction code</i>
FTP	<i>File transfer protocol</i>
IMAP	<i>Internet message access protocol</i>
IP	<i>Internet protocol</i>
IPv6	<i>Internet protocol version 6</i>
ISA	<i>Instruction set architecture</i>
JVM	<i>Java virtual machine</i>
KVM	<i>Kernel-based virtual machine</i>
LTS	<i>Long term support</i>
MTBF	<i>Mean time between failures</i>
MTTR	<i>Mean time to repair</i>
NAT	<i>Network address translation</i>
NRPE	<i>Nagios remote plugin executor</i>
PC	<i>Personal computer</i>
PHP	<i>Personal home page</i>
POP	<i>Post office protocol</i>
PPPoE	<i>Point-to-point protocol over ethernet</i>
PRTG	<i>Paessler router traffic grapher</i>
RAID	<i>Redundant array of independent disks</i>
SLA	<i>Service level agreement</i>
SMTP	<i>Simple mail transfer protocol</i>
SPOF	<i>Single point of failure</i>
SSH	<i>Secure shell</i>
SVN	<i>Subversion</i>
TI	<i>Tecnologia da Informação</i>
VM	<i>Virtual machine</i>
VMM	<i>Virtual machine monitor</i>
WHM	<i>WebHost manager</i>
XMPP	<i>Extensible messaging and presence protocol</i>

LISTA DE FIGURAS

Figura 3.1:	Interfaces de sistemas de computação.	15
Figura 3.2:	Máquinas virtuais de aplicação e de sistema.	16
Figura 3.3:	Componentes da virtualização.	17
Figura 3.4:	Arquiteturas de máquinas virtuais de sistema. COLOCAR host OS ABAIXO DO HIPERVISOR ???	18
Figura 3.5:	Implementações de máquinas virtuais de sistema.	19
Figura 4.1:	Diagrama de instalação elétrica.	23
Figura 4.2:	Imagem do <i>rack</i> e dos servidores.	24
Figura 4.3:	Modelo de estrutura física.	25
Figura 4.4:	Servidor de virtualização Brina. REFAZER ???	26
Figura 4.5:	Servidor de virtualização Fulmine.	28

LISTA DE TABELAS

Tabela 2.1: Níveis de alta disponibilidade e exemplos de sistemas	12
Tabela 4.1: Configuração dos servidores físicos.	25

RESUMO

Palavras-chave: Virtualização, Alta disponibilidade.

1 INTRODUÇÃO

O crescente avanço tecnológico e o desenvolvimento da internet, provocou um aumento no número de aplicações ou serviços que dependem da infraestrutura de Tecnologia da Informação (TI). Além disso, percebe-se um aumento significativo no número de operações e negócios *on-line* que são realizados, tanto por organizações públicas ou privadas, quanto por grande parte da população.

Desta forma, a sociedade está cada vez mais dependente da tecnologia, de computadores e de sistemas. De fato, pode-se observar sistemas computacionais desde em uma farmácia, até em uma grande indústria. Sendo assim, a estabilidade e a disponibilidade desses sistemas apresenta um grande impacto em nosso dia-a-dia, pois um grande número de atividades cotidianas dependem deles.

Uma interrupção imprevista em um ambiente computacional poderá causar um prejuízo financeiro para a empresa que fornece o serviço, além de interferir na vida das pessoas que dependem de forma direta ou indireta deste serviço. Essa interrupção terá maior relevância para as corporações cujo o serviço ou produto final é fornecido através da internet, como por exemplo, o comércio eletrônico, *web sites*, sistemas corporativos, entre outros. Em um ambiente extremo, pode-se imaginar o caos e o possível risco de perda de vidas que ocorreria em caso de uma falha em um sistema de controle aéreo (COSTA, 2009).

Para essas empresas um plano de contingência é fundamental para garantir uma boa qualidade de serviço, além de otimizar o desempenho das atividades, e também para fazer uma prevenção de falhas e uma recuperação rápida caso essas ocorram (COSTA, 2009). De fato, hoje em dia a confiança em um serviço é um grande diferencial para a empresa fornecedora deste serviço, sendo que a alta disponibilidade é fundamental para atingir este objetivo.

A alta disponibilidade consiste em manter um sistema disponível por meio da tolerância a falhas, isto é, utilizando mecanismos que fazem a detecção, mascaramento e a recuperação de falhas, sendo que esses mecanismos podem ser implementados a nível de *software* ou de *hardware* (REIS, 2009). Para que um sistema seja altamente disponível ele deve ser tolerante a falhas, sendo que a tolerância a falhas é frequentemente implementada, utilizando redundância. No caso de uma falha em um dos componentes evita-se a interrupção do sistema, uma vez que o sistema poderá continuar funcionando, utilizando o outro componente (BATISTA, 2007).

Neste trabalho será realizado um estudo sobre a implementação de um sistema de alta disponibilidade em uma empresa de hospedagens. Essa empresa oferece serviços pela internet, como por exemplo hospedagens de sites, *e-mail*, sistemas de gestão, *e-mail marketing*, entre outros. A empresa possui aproximadamente 60 servidores físicos e virtuais, e aproximadamente 9000 clientes, sendo que em períodos de pico

atende em torno de 1000 requisições por segundo.

Atualmente, a empresa possui redundância de conexões de acesso a internet, refrigeração e energia, com *nobreaks* e geradores. Porém, essa empresa não possui nenhuma redundância nos serviços que estão sendo executados nos servidores. Desta forma, caso ocorra uma falha de *software* ou de *hardware*, os serviços ficarão indisponíveis. Neste trabalho será realizada uma análise dos serviços oferecidos pela empresa, sendo que mecanismos de alta disponibilidade serão desenvolvidos para os serviços mais críticos. Para a redução dos custos serão utilizadas ferramentas gratuitas e de código aberto.

1.1 Objetivos

Atualmente a empresa estudada não possui nenhuma solução de alta disponibilidade para seus serviços críticos. Desta forma, neste trabalho será desenvolvida uma solução de alta disponibilidade para estes serviços, sendo que essa solução será baseada no uso de ferramentas de código aberto e de baixo custo. Para que o objetivo geral seja atendido os seguintes objetivos específicos deverão ser realizados:

- Identificar os serviços críticos a serem integrados ao ambiente de alta disponibilidade;
- Definir as ferramentas a serem utilizadas para implementar tolerância a falhas;
- Realizar testes para a validação do sistema de alta disponibilidade que foi desenvolvido.

1.2 Estrutura do trabalho

O trabalho foi estruturado em cinco capítulos, que são:

- Capítulo 2: apresenta o conceito de alta disponibilidade e conceitos relacionados;
- Capítulo 3: é apresentado um breve histórico da virtualização, bem como o conceito de máquinas virtuais e também as suas classificações e estratégias de implementação;
- Capítulo 4: descreve o ambiente atual da empresa, os serviços que são fornecidos e a identificação dos serviços críticos;
- Capítulo 5: apresenta a solução de alta disponibilidade utilizando virtualização no cenário da empresa.

2 ALTA DISPONIBILIDADE

Alta disponibilidade é uma técnica conhecida, sendo cada vez mais empregada em ambientes computacionais. O objetivo de prover alta disponibilidade resume-se em garantir que um serviço esteja sempre disponível quando o cliente solicitar ou acessar (COSTA, 2009). A alta disponibilidade geralmente é implementada com uma redundância de *hardware* ou de *software* para que o serviço fique mais tempo disponível, sendo que quanto maior for a disponibilidade desejada maior deverá ser a redundância no ambiente, assim reduzindo os pontos únicos de falha, que em inglês são chamados de *Single point of failure* (SPOF). A alta disponibilidade está diretamente relacionada aos conceitos de:

- Dependabilidade: indica a qualidade do serviço fornecido e a confiança depositada neste serviço. A dependabilidade envolve atributos como segurança de funcionamento, segurança de acesso, manutenabilidade, testabilidade e comprometimento do desempenho (WEBER, 2002);
- Confiabilidade: é o atributo mais importante, pois transmite a ideia de continuidade de serviço (PANKAJ, 1994). A confiabilidade refere-se a probabilidade de um serviço estar funcionando corretamente durante um dado intervalo de tempo;
- Disponibilidade: é a probabilidade de um serviço estar operacional no instante em que for solicitado (COSTA, 2009);
- Tolerância a falhas: procura garantir a disponibilidade de um serviço utilizando mecanismos capazes de detectar, mascarar e recuperar falhas. O seu principal objetivo é alcançar a dependabilidade, indicando uma boa qualidade de serviço (COSTA, 2009). A tolerância a falhas é um dos principais conceitos da alta disponibilidade, sendo descrita na Seção 2.1.

2.1 Tolerância a falhas

Sabe-se que o *hardware* tende a falhar, principalmente devido a fatores físicos, por isso utiliza-se métodos para a prevenção de falhas. A abordagem de prevenção de falhas é realizada na etapa de projeto, ou seja, consiste em definir mecanismos que impeçam que as falhas ocorram. Além disso, a prevenção de falhas melhora a disponibilidade e a confiabilidade de um serviço, uma vez que essa tem como objetivo diminuir a possibilidade de falhas antes de colocar o sistema em uso.

A prevenção de falhas não eliminará todas as possíveis falhas. Sendo assim, a tolerância a falhas procura fornecer a disponibilidade de um serviço mesmo com a presença de falhas. De fato, enquanto a prevenção de falhas tem foco nas fases de

projeto, teste e validação, a tolerância a falhas apresenta como foco a utilização de componentes replicados para mascarar as falhas (PANKAJ, 1994).

O objetivo da tolerância a falhas é aumentar a disponibilidade de um sistema, ou seja, aumentar o intervalo de tempo em que os serviços fornecidos estão disponíveis aos usuários. Um sistema é dito tolerante a falhas se ele for capaz de mascarar a presença de falhas ou recuperar-se de uma falha sem afetar o funcionamento do sistema.

A tolerância a falhas é implementada utilizando redundância (Seção 2.2). Um exemplo muito utilizado para tornar um sistema tolerante a falhas é a virtualização. Nestes ambientes normalmente existem dois servidores físicos onde máquinas virtuais são executadas, sendo que no caso de um dos servidores falhar, o *software* de monitoramento fará a transferência das máquinas virtuais para o outro servidor, de forma transparente aos usuários, evitando assim a indisponibilidade do serviço. Os principais conceitos de virtualização, são apresentados no Capítulo 3.

A tolerância a falhas pode ser dividida em dois tipos. O primeiro tipo, o mascaramento, não se manifesta na forma de erro ao sistema, pois as falhas são tratadas na origem. O mascaramento é utilizado principalmente em sistemas de tempo real crítico. Um exemplo são os códigos de correção de erros, em inglês *Error correction code* (ECC), que são utilizados em memórias para detecção e correção de erros.

O segundo tipo consiste em detectar, localizar a falha, e reconfigurar o *software* ou *hardware* de forma a corrigir a falha. Esse tipo de tolerância a falha é dividido nas seguintes etapas (WEBER, 2002).

- Detecção: realiza o monitoramento e aguarda uma falha se manifestar em forma de erro, para então passar para a próxima fase. Um exemplo de detecção de erro é um cão de guarda (*watchdog timer*), que recebe um sinal do programa ou serviço que está sendo monitorado e caso este sinal não seja recebido, o *watchdog* irá se manifestar na forma de erro. Um outro exemplo é o esquema de duplicação e comparação, onde são realizadas operações em componentes replicados com os mesmos dados de entrada, e então os dados de saída são comparados. No caso de diferenças nos dados de saída um erro é gerado.
- Confinamento: responsável pela restrição de um erro para que dados inválidos não se propaguem para todo o sistema, pois entre a falha e a detecção do erro há um intervalo de tempo. Neste intervalo pode ocorrer a propagação do erro para outros componentes do sistema, sendo assim antes de executar medidas corretivas é necessário definir os limites da propagação. Na fase de projeto essas restrições devem ser previstas e tratadas. Um exemplo de confinamento é o isolamento de alguns processos que estão em execução em um sistema operacional, sendo que esse sistema faz o gerenciamento dos processos para isolar e impedir que as falhas de um processo gerem problemas em outros processos.
- Recuperação: após a detecção de um erro ocorre a recuperação, onde o estado de erro é alterado para estado livre de erros. A recuperação pode ser feita de duas formas, que são:
 - *forward error recovery* (recuperação por avanço): ocorre uma condução para um estado que ainda não ocorreu. É a forma de recuperação mais eficiente, porém mais complexa de ser implementada.
 - *backward error recovery* (recuperação por retorno): ocorre um retorno

para um estado anterior e livre de erros. Para retornar ao estado anterior podem ser utilizados pontos de recuperação (*checkpoints*). Assim quando ocorrer um erro, um *rollback* é executado, ou seja, o sistema retornará a um estado anterior a falha.

- **Tratamento:** procura prevenir que futuros erros aconteçam. Nesta fase ocorre a localização da falha para descobrir o componente que originou a falha. A substituição do componente danificado pode ser feita de forma manual ou automática. O reparo manual é feito por um operador que é responsável pelo reparo ou substituição de um componente. Como exemplo pode-se citar a troca de um disco rígido de um servidor. Já o reparo automático é utilizado quando existe um componente em espera para a substituição, como por exemplo, um disco configurado como *hot spare*, ou seja, um componente de *backup* que assumirá o lugar do outro imediatamente após o componente principal falhar. Em *storages* ou servidores, o *hot spare* pode ser configurado através de um *Redundant array of independent disks* (RAID) (ROUSE, 2013).

2.2 Redundância

A redundância pode ser implementada através da replicação de componentes, e apresenta como objetivo reduzir o número de SPOF e garantir o mascaramento de falhas. Na prática, se um componente falhar ele deve ser reparado ou substituído por um novo, sem que haja uma interrupção no serviço. Além disso, a redundância pode ser implementada através do envio de sinais ou *bits* de controle junto aos dados, servindo assim para detecção e correção de erros (WEBER, 2002). Segundo (NØRVÅG, 2000) existem quatro tipos diferentes de redundância que são:

- **Hardware:** utiliza-se a replicação de componentes, sendo que no caso de falha em um deles o outro possa assumir seu lugar. Para fazer a detecção de erros a saída de cada componente é constantemente monitorada e comparada à saída do outro componente. Um exemplo prático de redundância de *hardware* são os servidores com fontes redundantes. Neste caso são utilizadas duas fontes ligadas em paralelo, sendo que caso uma falhe a outra suprirá a necessidade de todo o servidor;
- **Informação:** ocorre quando uma informação extra é enviada ou armazenada para possibilitar a detecção e a correção de erros. Um exemplo são os *checksums* (soma de verificação). Esses são calculados antes da transmissão ou armazenamento dos dados e recalculados ao recebê-los ou recuperá-los, assim sendo possível verificar a integridade dos dados. Outro exemplo bastante comum são os *bits* de paridade que são utilizados para detectar falhas que afetam apenas um *bit* (WEBER, 2002);
- **Software:** pode-se definir redundância de *software* como a configuração de um serviço ou *software* em dois ou mais locais diferentes. Pode-se citar como exemplo, um sistema gerenciador de banco de dados *MySQL*, que pode ser configurado com um modelo de replicação do tipo *master-slave*, onde um servidor principal (*master*) grava as operações em um arquivo, para que então os servidores *slaves*, possam recuperar e executar essas operações, com isso mantendo os dados sincronizados. Neste caso, tanto o servidor *master* quanto os *slaves*

Nível	Uptime	Downtime por ano	Exemplos
1	90%	36.5 dias	computadores pessoais
2	98%	7.3 dias	
3	99%	3.65 dias	sistemas de acesso
4	99.8%	17 horas e 30 minutos	
5	99.9%	8 horas e 45 minutos	provedores de acesso
6	99.99%	52.5 minutos	CPD, sistemas de negócios
7	99.999%	5.25 minutos	sistemas de telefonia ou bancários
8	99.9999%	31.5 minutos	sistemas de defesa militar

Tabela 2.1: Níveis de alta disponibilidade e exemplos de sistemas

executam o serviço *MySQL*, caracterizando uma redundância (SILVA VIANA, 2015). A redundância de *software* também pode ser implementada com o objetivo de tolerar falhas e *bugs* em um *software* crítico. Existem algumas técnicas que podem ser utilizadas para isso, como por exemplo, a programação de *n*-versões, que consiste no desenvolvimento de *n* versões de um mesmo *software*, desta forma, possibilita-se o aumento da disponibilidade, uma vez que elas provavelmente não apresentarão os mesmos erros. A programação de *n*-versões possui um custo muito elevado, não sendo muito utilizada.

- Tempo: este é feito através da repetição de um conjunto de instruções em um mesmo componente, assim detectando uma falha caso ocorra. Essa técnica necessita tempo adicional, e é utilizada em sistemas onde o tempo não é crítico. Por exemplo, um *software* de monitoramento de serviços que faz um teste em cada serviço. No caso de ocorrência uma falha em um serviço, uma ação corretiva será executada para reestabelecer este serviço. Essa técnica, diferentemente da redundância de *hardware*, não requer um *hardware* extra para sua implementação (COSTA, 2009).

2.3 Cálculo da alta disponibilidade

Um aspecto importante sobre alta disponibilidade é como medi-la. Para isso são utilizados os valores de *uptime* e *downtime*, que são respectivamente, o tempo em que os serviços estão em execução e o tempo em que não estão executando. A alta disponibilidade pode ser expressa pela quantidade de “noves”, isto é, se um serviço possui quatro noves de disponibilidade, este possui uma disponibilidade de 99,99% (PEREIRA FILHO, 2004).

A Tabela 2.1 apresenta alguns níveis de disponibilidade, e os seus percentuais de *Uptime*, os *Downtime* por ano. Já na última coluna tem-se alguns exemplos de serviços relacionados ao nível de disponibilidade. Pode-se observar que para alguns serviços, como por exemplo, sistemas bancários ou sistemas militares é necessário um alto nível de disponibilidade (PEREIRA FILHO, 2004).

A porcentagem de disponibilidade (*d*) pode ser calculada através da equação

$$d = \frac{MTBF}{(MTBF + MTTR)} \quad (2.1)$$

onde *Mean time between failures* (MTBF) corresponde ao tempo médio entre falhas, ou seja, corresponde ao tempo médio entre as paradas de um serviço. Já o *Mean time to repair* (MTTR) é o tempo médio de recuperação, isto é, o tempo entre a queda e a recuperação de um serviço (GONÇALVES, 2009).

A alta disponibilidade é um dos principais fatores que fornece confiança aos clientes ou usuários de um serviço, sendo extremamente importante em empresas que fornecem serviços *on-line*. Por isso, as empresas desenvolveram o *Service level agreement* (SLA), que é um acordo de nível de serviço, que garante que o serviço fornecido atenda as expectativas dos clientes. Um SLA é um documento contendo uma descrição e uma definição das características mais importantes do serviço que será fornecido. Esse acordo apresenta também o percentual de disponibilidade do serviço. Além disso, um SLA deverá conter descrição do serviço, requerimentos, horário de funcionamento, *uptime* do serviço, *downtime* máximo do serviço, entre outros (SMITH, 2010).

2.4 Considerações finais

Neste capítulo foram descritos os principais conceitos de alta disponibilidade e conceitos relacionados. Como mencionado anteriormente, um dos principais recursos utilizados para a obtenção de alta disponibilidade é a virtualização, uma vez que essas são utilizadas para implementar a redundância de *software*. Desta forma, no próximo capítulo será feita uma breve definição de virtualização, com as vantagens e as estratégias de implementação de máquinas virtuais.

3 VIRTUALIZAÇÃO

O conceito virtualização surgiu na década de 60, onde muitas vezes era necessário que um usuário utilizasse um ambiente individual, com suas próprias aplicações e totalmente isolado dos demais usuários. Esse foi um dos principais motivos para a criação das máquinas virtuais, que eram conhecidas como *Virtual machine* (VM). As VMs apresentaram uma forte expansão com o sistema operacional *370*, que foi desenvolvido pela *IBM*, e foi um dos principais sistemas comerciais com suporte à virtualização da época. Esse sistema operacional executava em *mainframes*, que eram grandes servidores capazes de processar um grande volume de informações (LAUREANO; MAZIERO, 2008).

Na década de 80 houve uma redução no uso da virtualização devido a popularização do *Personal computer* (PC). Na época era mais vantajoso disponibilizar um PC para cada usuário, do que investir em *mainframes*. Devido à crescente melhora na performance do PC e ao surgimento da linguagem *Java*, no início da década de 90, a tecnologia de virtualização retornou com o conceito de virtualização de aplicação.

A virtualização foi definida nos anos 60 e 70 como uma camada entre o *hardware* e o sistema operacional que possibilitava a divisão e a proteção dos recursos físicos. Porém, atualmente ela abrange outros conceitos, como por exemplo a *Java virtual machine* (JVM), que não virtualiza um *hardware*. De fato, essa permite que uma aplicação convidada execute em diferentes tipos de sistemas operacionais.

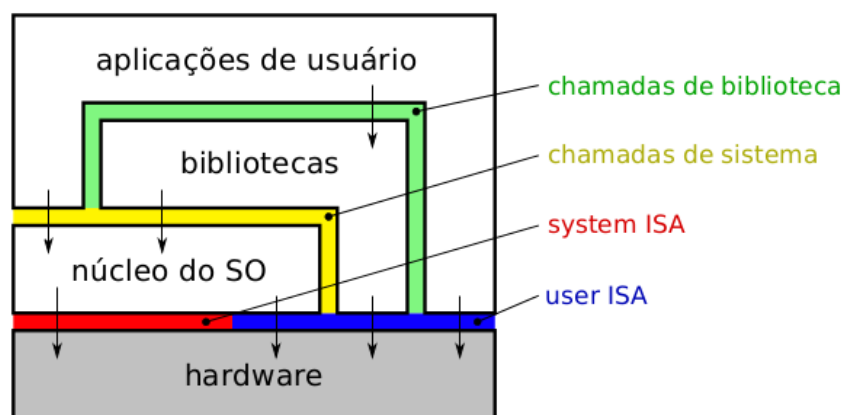
Atualmente, define-se virtualização como uma camada de *software* que utiliza os serviços fornecidos por uma determinada interface de sistema para criar outra interface de mesmo nível. De fato, essa camada permite a comunicação entre interfaces distintas, de forma que uma aplicação desenvolvida para uma plataforma *X* possa também executar em uma plataforma *Y* (LAUREANO; MAZIERO, 2008).

Como mencionado, a virtualização permite a comunicação entre diferentes interfaces, sendo que existem diferentes tipo de interfaces em sistemas de computação (Figura 3.1) (MAZIERO, 2013):

- Conjunto de instruções ou *Instruction set architecture* (ISA): é a interface básica, que fica entre o *software* e o *hardware*, e é composta por instruções de código de máquina. Essa interface é dividida em dois grupos:
 - Instruções de usuário ou *User ISA*: são instruções disponíveis às aplicações de usuários. Essas instruções executam em modo usuário, sendo que nesse modo há restrição para controle dos recursos de *hardware*. Instruções de usuário são instruções não privilegiadas, ou seja, são instruções que podem ser executadas sem interferir em outras tarefas, porque elas não

acessam recursos compartilhados. Este grupo de interface contém, por exemplo, instruções de operações aritméticas e instruções de ponto flutuante; (BUYA; VECCHIOLA; SELVI, 2013);

- Instruções de sistema ou *System ISA*: essas instruções geralmente são disponibilizadas para o núcleo do sistema operacional. Elas são instruções privilegiadas, ou seja, são instruções que acessam recursos compartilhados. Essas instruções são executadas em modo supervisor (ou modo *kernel*), que permitem realizar operações sensíveis¹ no *hardware* (BUYA; VECCHIOLA; SELVI, 2013). Pode-se citar as instruções que alteram o estado dos registradores do processador como exemplo de instruções de sistema;
- Chamadas de sistema ou *syscalls*: são operações oferecidas pelo núcleo do sistema operacional para as aplicações dos usuários. Essas operações permitem um acesso controlado aos dispositivos, memória e processador. As instruções privilegiadas não podem ser executadas no modo usuário, por isso, as aplicações de usuários utilizam chamadas de sistemas em seu lugar, e então o sistema operacional determina se essas operações não irão comprometer a integridade do sistema (MARINESCU, 2013). Um exemplo de chamada de sistema é uma operação de escrita em disco ou qualquer operação de entrada e saída feito por aplicações de usuários.

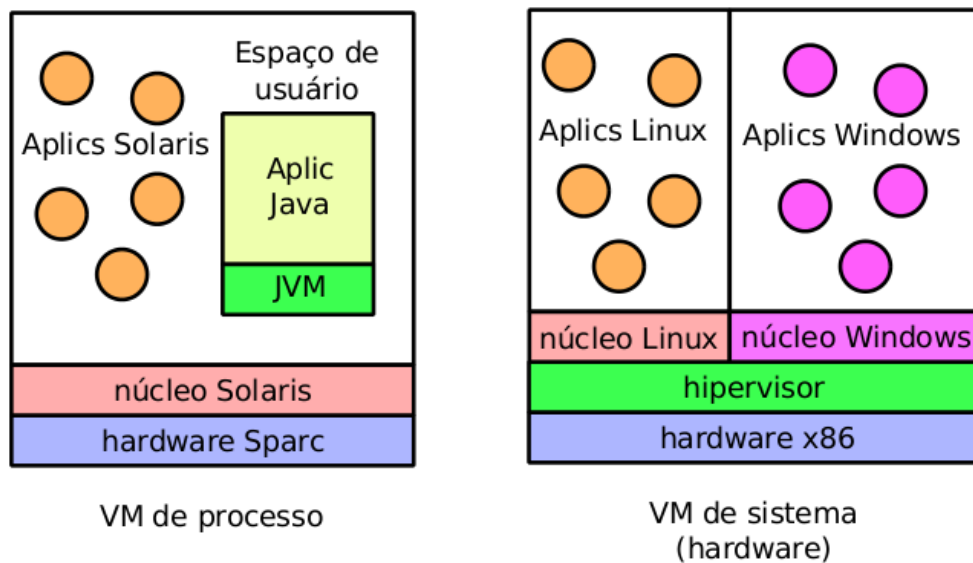


Fonte: MAZIERO (2013)

Figura 3.1: Interfaces de sistemas de computação.

Máquinas virtuais podem ser divididas em dois grupos principais, que são: as máquinas virtuais de aplicação (Seção 3.1), e máquinas virtuais de sistema (Seção 3.2). As máquinas virtuais de aplicação fazem a virtualização de uma aplicação e suportam apenas uma aplicação, ou seja, elas provêm um ambiente que permite a execução de uma aplicação convidada. Um exemplo de máquina virtual de aplicação é a JVM. Já uma máquina virtual de sistema suporta um sistema operacional convidado, com suas aplicações executando sobre ele (Figura 3.2). Uma máquina virtual executando sobre o hipervisor *Kernel-based virtual machine* (KVM) é um exemplo de máquina virtual de aplicação (LAUREANO; MAZIERO, 2008).

¹Operações sensíveis são operações que podem alterar o estado do processador.



Fonte: LAUREANO; MAZIERO (2008)

Figura 3.2: Máquinas virtuais de aplicação e de sistema.

3.1 Máquinas virtuais de aplicação

As máquinas virtuais de aplicação, também chamadas de máquinas virtuais de processos, são responsáveis por prover um ambiente que permite a execução de uma aplicação convidada, sendo que esta aplicação possui um conjunto de instruções, ou de chamadas do sistema, diferentes da arquitetura do sistema hospedeiro. Neste caso, quando temos chamadas do sistema operacional ou instruções de máquina, será necessário uma tradução dessas interfaces, que será feita pela camada de virtualização. Os dois principais tipos de máquinas virtuais de aplicação são:

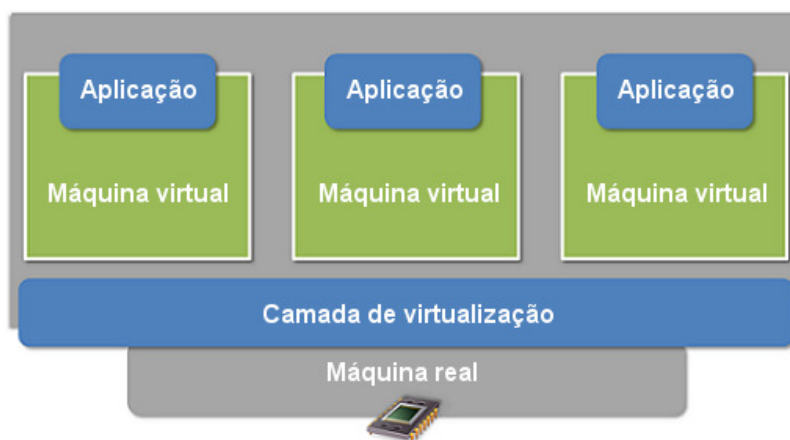
- Máquinas virtuais de linguagem de alto nível: esse tipo de máquina virtual foi criado levando em consideração uma linguagem de programação e o seu compilador. Neste caso, o código compilado gera um código binário que não pode ser executado em uma arquitetura real, mas pode ser executado em uma máquina virtual. Sendo assim para cada arquitetura ou sistema operacional deverá existir uma máquina virtual que permita a execução da aplicação. Como exemplo deste tipo de máquina virtual pode-se citar a máquina virtual Java (JVM) e a *Microsoft Common Language Infrastructure*, que é a base da plataforma *.NET* (CARISSIMI, 2008);
- Emulação no sistema operacional: nesse caso é feito um mapeamento entre as chamadas de sistema que são utilizadas pela aplicação e as chamadas do sistema operacional real. A virtualização de aplicação pode ser encontrada em ferramentas que emulam uma aplicação que foi desenvolvida para uma plataforma em uma outra plataforma. Como exemplo, pode-se citar o *Wine* (WineHQ, 2016), que permite executar aplicações *Windows* em plataformas *Linux*.

3.2 Máquinas virtuais de sistema

As máquinas virtuais de sistema, também chamadas de hipervisor ou *Virtual machine monitor* (VMM), são uma camada de *software* que possibilita que um ou mais sistemas operacionais convidados executem sobre um mesmo computador físico, ou seja, o hipervisor provê uma interface ISA virtual, que pode ou não ser igual a interface real, e virtualiza outros componentes de *hardware*, para que cada máquina virtual convidada possa ter seus próprios recursos. Para tanto, a virtualização de sistema utiliza abstrações em sua arquitetura. Por exemplo, ela transforma um disco rígido físico em dois discos rígidos virtuais menores, sendo que esses discos virtuais são arquivos armazenados no disco físico (SMITH; NAIR, 2005).

Nesse modelo, o ambiente de virtualização de sistema é composto basicamente por três componentes (Figura 3.3):

- Máquina real: também chamado de hospedeiro, que é o *hardware* onde o sistema de virtualização irá executar;
- Camada de virtualização: é conhecida como hipervisor ou também chamada de VMM. Essa camada tem como função criar interfaces virtuais, para a comunicação da máquina virtual com a máquina real;
- Máquina virtual: também conhecido como sistema convidado, que executa sobre a camada de virtualização. Geralmente, tem-se várias máquinas virtuais executando simultaneamente sobre esta camada.



Fonte: ANDRADE (2011)

Figura 3.3: Componentes da virtualização.

3.2.1 Arquiteturas de máquinas virtuais de sistema

Existem basicamente duas arquiteturas de hipervisor de sistema, que são apresentadas na Figura 3.4 (MAZIERO, 2013):

- Hipervisores nativos: esse hipervisor executa diretamente sobre o *hardware*, ou seja, sem um sistema operacional hospedeiro. Neste caso, o hipervisor nativo faz a multiplexação dos recursos do *hardware* (memória, disco rígido, interface de rede, entre outros) e disponibiliza esses recursos para as máquinas virtuais. Alguns exemplos que utilizam esse hipervisor são *IBM 370* (IBM, 2016), o



Fonte: MAZIERO (2013)

Figura 3.4: Arquiteturas de máquinas virtuais de sistema. COLOCAR host OS ABAIXO DO HIPERVISOR ???

Xen (Citrix, 2016a) e o *VMware ESXi* (VMware, 2016a);

- Hipervisores convidados: esse tipo de hipervisor executa sobre um sistema operacional hospedeiro e utiliza os recursos desse sistema para gerar recursos para as máquinas virtuais. Normalmente esse tipo suporta apenas um sistema operacional convidado para cada hipervisor. Exemplos de *softwares* que possuem esse tipo de arquitetura são: o *VirtualBox* (Oracle, 2016), o *VMware Player* (VMware, 2016b) e o *QEmu* (QEmu, 2016).

Destaca-se que hipervisores convidados são mais flexíveis que os nativos, pois podem ser facilmente instalados ou removidos de um sistema operacional existente. Já os hipervisores nativos possuem melhor desempenho pois acessam o *hardware* diretamente.

3.2.2 Implementações de máquinas virtuais de sistema

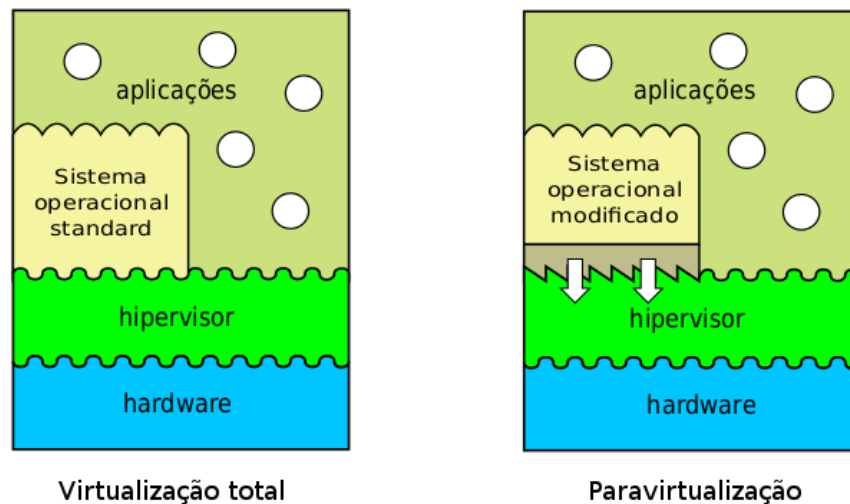
As máquinas virtuais de sistema podem ser implementadas usando diferentes estratégias. Atualmente as estratégias mais utilizadas são a virtualização total e a paravirtualização (Figura 3.5):

- Virtualização total: nesta estratégia todas as interfaces de acesso ao *hardware* são virtualizadas. Desta forma, possibilita-se que os sistemas operacionais convidados executem como se estivessem diretamente sobre o *hardware*. Na virtualização total o conjunto de instruções do processador é acessível somente pelo hipervisor, sendo que essa estratégia utiliza tradução dinâmica² para traduzir as instruções do sistema convidado. A grande vantagem dessa estratégia é a possibilidade de um sistema convidado ser executado sem a necessidade de

²A tradução dinâmica analisa e reorganiza as instruções de um sistema convidado para melhorar o desempenho da execução, além disso a tradução dinâmica adapta as instruções do sistema convidado para o sistema real.

ser modificado. Porém, essa estratégia possui um desempenho inferior devido ao fato do hipervisor intermediar todas as chamadas de sistemas e operações do sistema convidado. Um exemplo ferramenta que utiliza virtualização total é o *QEmu* (QEmu, 2016);

- Paravirtualização: esta estratégia de implementação utiliza arquitetura de hipervisor nativo. Para melhorar o desempenho da virtualização foi modificado a interface entre o hipervisor e o sistema operacional convidado, com isso obteve-se um melhor acoplamento entre o sistema convidado e o hipervisor. As modificações na interface de sistema (*system ISA*) exigem que o sistema operacional convidado seja adaptado para o hipervisor, para possibilitar a execução sobre a plataforma virtual. Para esse acoplamento, o hipervisor disponibiliza uma *Application programming interface* (API), para que os sistemas convidados possam acessar o ISA de sistema. Contudo, a interface de usuário é mantida, assim as aplicações do sistema convidado não necessitam ser modificadas (MAZIERO, 2013).



Fonte: MAZIERO (2013)

Figura 3.5: Implementações de máquinas virtuais de sistema.

A paravirtualização possui um desempenho superior se comparada a virtualização total, pois acessa alguns recursos de forma direta, sendo que o hipervisor é responsável somente por impedir que o sistema convidado execute operações indevidas. Pode-se citar como exemplo o controle de acesso à memória feito pelo hipervisor. Na virtualização total o hipervisor reserva um espaço para cada sistema convidado, que por sua vez acessa a memória como se fosse uma memória física (que inicia o seu endereçamento na posição zero). Sendo assim, cada vez que o sistema convidado acessar a memória, o hipervisor precisará converter os endereços do sistema convidado para os endereços reais de memória. Já na paravirtualização, o hipervisor informa ao sistema convidado a área de memória que ele pode utilizar, assim não sendo necessário nenhuma conversão de endereços.

Apesar de apresentar um desempenho inferior, a virtualização total possui uma maior portabilidade, ou seja, permite que sistemas operacionais executem como convidados, sem a necessidade de serem modificados. Assim pode-se, por exemplo, transferir um sistema operacional instalado diretamente em uma máquina física

para um ambiente virtual, sem a necessidade de reinstalá-lo e reconfigurar todas as aplicações.

3.3 Vantagens das máquinas virtuais

De modo geral, a principal vantagem das máquinas virtuais de aplicação é a possibilidade de um mesmo código executável funcionar em diversos sistemas operacionais. Já para máquinas virtuais de sistema, destaca-se a possibilidade de executar mais de um sistema operacional sobre um mesmo *hardware*. Nas próximas seções será descrito as principais utilizações e vantagens de máquinas virtuais de *desktops* e de servidores.

3.3.1 Virtualização de Desktop

A portabilidade é uma das grandes vantagens da virtualização, que também pode ser aplicada em *desktops*. Pode-se citar como exemplo o desenvolvimento de *software* para diversos sistemas operacionais sem a necessidade de aquisição de um computador físico para cada sistema operacional. Assim, máquinas virtuais em *desktops* podem ser utilizadas em ambientes de desenvolvimento, pois possibilitam a execução de múltiplas plataformas sem comprometer o sistema operacional original (CARIS-SIMI, 2008). Um exemplo é o *VMware Workstation*, que possibilita a virtualização em PC para fins de desenvolvimento de *software* (VMware, 2016).

Em empresas pode-se utilizar virtualização de *desktops*, através da configuração de terminais remotos nos computadores e um servidor para centralizar as máquinas virtuais. Com isso torna-se mais simples a manutenção dos *desktops* e exige um *hardware* de menor valor, uma vez que esses executarão apenas um terminal remoto. Além disso essa técnica possibilita uma maior segurança dos dados, pois os dados serão armazenados em um local seguro, como um datacenter por exemplo. Exemplos desse tipo de virtualização são o *Xen Desktop* (Citrix, 2016b) e o *VMware Horizon View* (VMware, 2016c).

Para usuários de computadores em geral a virtualização é importante também, algumas vezes precisa-se utilizar ou testar *softwares* que não estão disponíveis para a plataforma utilizada, deste modo a virtualização possibilita executar qualquer sistema operacional no computador do usuário, sem a necessidade de reiniciá-lo. Por exemplo, para usuários *Linux* é comum precisar executar aplicações que não existem para sua plataforma, sendo assim necessário utilizar uma máquina virtual *Windows* para isso.

Pode-se também encontrar virtualização de *desktops* em laboratórios de ensino, devido a necessidade de executar diferentes sistemas operacionais para determinadas disciplinas. Isso é necessário quando pretende-se configurar e executar aplicações para fim de experimentos ou aprendizagem, com isso, essas ações não afetarão o sistema hospedeiro, pois estarão executando no sistema operacional de uma máquina virtual. A grande vantagem da utilização de máquinas virtuais nesse tipo de ambiente é a facilidade na manutenção, pois as máquinas virtuais podem ser restauradas de uma forma simples.

3.3.2 Virtualização de servidores

Em muitos casos as empresas utilizam serviços distribuídos entre diferentes servidores físicos, como, por exemplo, servidores de e-mail, hospedagens e banco de dados,

isso faz com que alguns recursos fiquem ociosos, pois muitas vezes um serviço utiliza mais um recurso do que outro, por exemplo um serviço pode utilizar muito acesso a disco, por outro lado utilizar pouca memória, assim nesse servidor a memória se torna ociosa. Portanto, uma das grandes vantagens da virtualização é um melhor aproveitamento dos recursos. De fato, alocando vários serviços em um único servidor físico tem-se um melhor aproveitamento do *hardware* (MOREIRA, 2006). E consequentemente tem-se uma redução de custos com a administração e a manutenção dos servidores físicos.

Em um ambiente heterogêneo pode-se também utilizar virtualização, pois ela permite a instalação de diversos sistemas operacionais em um único servidor. Esse tipo de virtualização favorece a implementação do conceito “um servidor por serviço”, que consiste em ter um servidor para cada serviço. Além disso, tem-se o isolamento de serviços, ou seja, caso ocorra uma falha de segurança em um serviço, essa falha não comprometerá todo o sistema, pois cada serviço estará executando em seu próprio sistema operacional (CARISSIMI, 2008).

Outra motivação para a utilização de virtualização consiste na redução de custos em energia elétrica, espaço físico e equipe. Essa redução de custos pode ser obtida através da implantação de servidores mais robustos para substituir dezenas de servidores comuns. Outro fator como a refrigeração do ambiente também pode ser reduzido com a implantação de virtualização de servidores, que consequentemente reduz o custo de energia.

A vantagem que fará parte da implementação deste trabalho é a migração em tempo real, mais conhecida como *live migration*. Nessa técnica existe a possibilidade de uma máquina virtual, que esta executando em um *hardware*, ser transferida através da rede para outro *hardware* sem ser reiniciada. Nesse processo a máquina fica no estado suspenso (por um período bem curto de tempo) até que o *hardware* de destino receba os dados necessários para continuar a execução da máquina virtual (SILVA, 2009).

3.4 Considerações finais

Neste capítulo foi apresentado um breve histórico e os dois principais grupos de máquinas virtuais que são: máquinas virtuais de aplicação e máquinas virtuais de sistema. Também foram apresentadas as vantagens e as estratégias de implementação de máquinas virtuais de sistema, dando ênfase para as máquinas virtuais de sistema, uma vez que essas são o foco deste trabalho. De fato, essas serão o tipo de redundância de *software* que será utilizada neste trabalho. No próximo capítulo será feito o levantamento e análise dos serviços fornecidos pela empresa, e posteriormente a seleção dos serviços mais críticos para possibilitar a implementação da solução de alta disponibilidade.

4 ESTUDO DE CASO

Neste capítulo será apresentada a estrutura de uma empresa que fornece serviços de hospedagens e também está associada a um provedor de internet¹. A empresa possui grande parte de seus clientes localizados na serra do Rio Grande do Sul, sendo que atualmente essa empresa possui aproximadamente 9000 clientes. A sede da empresa está localizada na cidade de Garibaldi, além disso possui quatro filiais no estado, atendendo aproximadamente xx?? cidades. Essa empresa possui aproximadamente xx?? funcionários.

A empresa oferece serviços pela internet aos seus clientes, que são: hospedagens de sites, banco de dados, *e-mail*, sistemas de gestão, *e-mail marketing*, *backup*, *máquinas virtuais*, autenticação *Asymmetric Digital Subscriber Line* (ADSL), rádio *online* e telefonia. Além disso, o provedor associado fornece aos seus clientes acesso à internet via rádio e acesso à internet por meio de fibra óptica. A maioria dos serviços são fornecidos por meio de *softwares* de código aberto, que executam sobre sistemas operacionais, normalmente distribuições *Linux*, e também são *softwares* livre.

Atualmente a empresa possui redundância de refrigeração e de energia (Figura 4.1). A redundância de refrigeração é composta por dois ares-condicionados. A redundância de energia é feita através de três *nobreaks*, sendo que dois deles são utilizados para alimentação dos servidores e outros equipamentos como por exemplo roteadores, de uma forma que caso um falhar o outro alimente todos os equipamentos. O terceiro *nobreak* é utilizado para alimentar os computadores dos funcionários de dois setores. Além disso, dois geradores suprem a necessidade de consumo de energia elétrica do ambiente.

Nas próximas seções serão detalhados: o ambiente físico dos servidores, com suas estruturas e suas configurações, além da estrutura de virtualização e todos os serviços fornecidos pelos servidores (Seção 4.1), e por fim, a seleção dos serviços críticos (Seção 4.2).

4.1 Ambiente físico e virtual

A estrutura atual da empresa é composta por quatorze servidores físicos montados em um *rack* (Figura 4.2). A configuração de *hardware* desses servidores encontradas na Tabela 4.1, onde tem-se o nome do servidor, o modelo do servidor, a configuração dos processadores, quantidade de memória, número de discos e a capacidade unitária de cada disco.

¹É importante salientar que esse provedor utiliza a maior parte dos serviços da empresa, pois possui maior número de clientes.

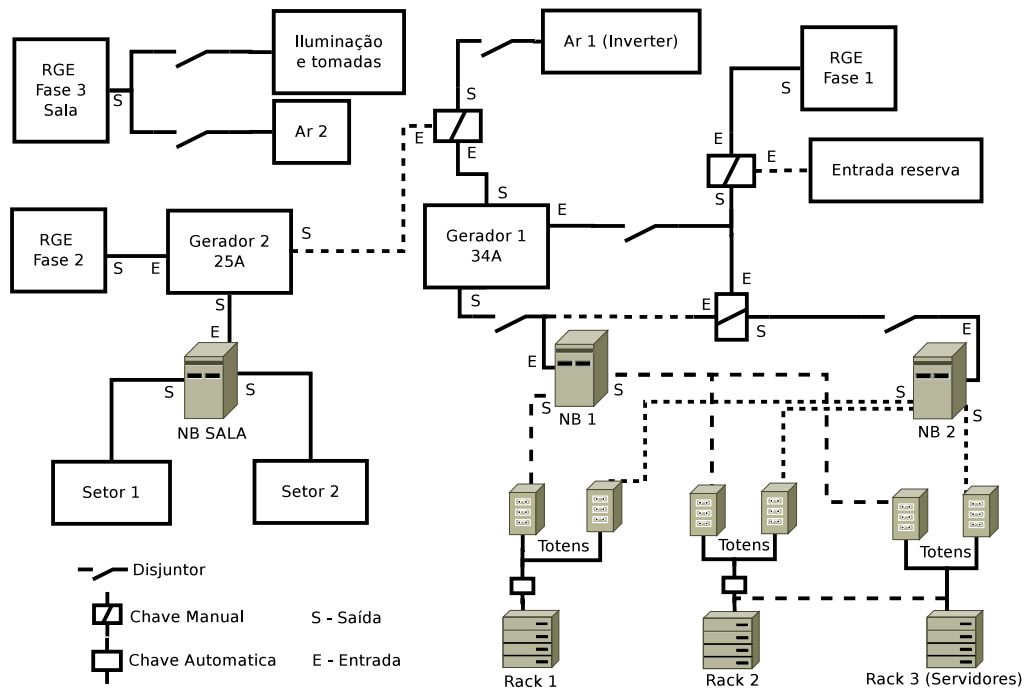


Figura 4.1: Diagrama de instalação elétrica.

Todos os servidores estão ligados ao *switch*, que provê aos servidores acesso à internet através do roteador. Para os servidores mais importantes utiliza-se dois cabos de rede que estão ligados a um *switch gigabit*, assim possibilitando a configuração de *link aggregation*, que possibilita configurar mais de uma interface de rede física em uma interface agregada, com isso permitindo dobrar a capacidade de tráfego de dados e assim é caracterizado a redundância do cabeamento. O diagrama da Figura 4.3 demonstra uma visão geral da estrutura física dos servidores da empresa, com dois exemplos de cada tipo de servidor.

Existem sete servidores que possuem serviços executando sobre o sistema operacional nativo, ou seja, sem virtualização. Eles são os sete primeiros servidores da Tabela 4.1:

- Bello: esse servidor possui o sistema operacional *Ubuntu 14.04 Long term support (LTS)*. Sua função é armazenar dados de *backup*, ele possui *storage* da ferramenta *Bacula 5.2.6* (pacote *bacula-sd 5.2.6*) para *backup* dos outros servidores;
- Cacti: um dos servidores de monitoramento da rede do provedor. Esse utiliza a distribuição *CentOS 6.6* e executa a aplicação *Cacti 0.8.8b*, que é uma ferramenta de código aberto desenvolvida para monitorar equipamentos de rede. Ela monitora atualmente a maior parte da rede *core* e a rede *backbone* tanto dos clientes de internet via rádio, como de fibra óptica;
- Dati: é o servidor de banco de dados principal. Esse possui o sistema operacional *Ubuntu 14.04 LTS*. O serviço que executa sobre esse servidor é um sistema gerenciador de banco de dados *MySQL 5.5.49*, onde armazena os dados das aplicações de *ZoneMinder* (servidor de câmeras) e *Icewarp Server* (servidor de e-mail), que serão detalhados posteriormente;
- Monit: esse servidor faz o monitoramento de todos os servidores. Ele possui o sistema operacional *Ubuntu 12.04 LTS*. Suas aplicações são *Nagios 3.2.3* e



Figura 4.2: Imagem do *rack* e dos servidores.

Munin 1.4.6, ambos *softwares* livres. O primeiro monitora desde os serviços de cada servidor, até o seu *hardware*, para isso utiliza um cliente (*Nagios remote plugin executor* (NRPE) 2.12), que deve ser instalado em cada servidor, para monitorar dados não acessíveis externamente, como espaço em disco, número de processos, falhas de *hardware*, entre outros. O segundo, *Munin*, é responsável por gerar gráficos para ajudar com monitoramento, com ele pode-se criar por exemplo gráfico de processador, memória, utilização de disco, e até temperatura e velocidade dos *fans* para alguns servidores;

- Nino: esse é o servidor utilizado pelo setor de desenvolvimento de *software*. Suas aplicações executam sobre o sistema operacional *Ubuntu 14.04 LTS*. Os serviços fornecidos pelo servidor são: servidor *web* (*Apache 2.4.7* e *Personal home page (PHP) 5.5.9*), sistema gerenciador de banco de dados (*MySQL 5.5.49* e *PostgreSQL 9.3.13*), compartilhamento de arquivos (*Samba 4.3.9*),

Servidor	Modelo	Processador	Memória	Disco
Bello		1 x Intel Core 2 Duo CPU E6750 2.66 GHz	2 GB DDR2	5,5 TB SATA
Cacti	Dell PowerEdge 2950	2 x Intel Xeon CPU E5310 1.60 GHz	12 GB DDR2	2 x 73 GB SAS
Dati	Dell PowerEdge 1850	2 x Intel Xeon CPU 3.20 GHz	4 GB DDR2	2 x 146 GB SCSI
Monit		1 x Intel Core 2 Quad CPU Q9550 2.83 GHz	4 GB DDR2	120 GB SSD
Nino		1 x Intel Core 2 Duo CPU E4500 2.20 GHz	4 GB DDR2	500 GB SATA
Sfrunhon		1 x Intel Xeon CPU X3330 2.66 GHz	8 GB DDR2	750 GB SATA
Vigilante		1 x Intel Pentium Dual CPU E2180 2.00 GHz	4 GB DDR2	2,5 TB SATA
Brina	Dell PowerEdge 2950	2 x Intel Xeon CPU E5410 2.33 GHz	24 GB DDR2	6 x 300 GB SAS
Fulmine	IBM System x3650 M4	1 x Intel Xeon CPU E5-2650 2.00 GHz	32 GB DDR3	6 x 2 TB SATA
Piova	Dell PowerEdge R410	2 x Intel Xeon CPU E5530 2.40 GHz	32 GB DDR3	4 x 500G SATA
Raggio	HP ProLiant DL360 G7	2 x Intel Xeon CPU E5630 2.53 GHz	32 GB DDR3	4 x 300 GB SAS
Tempesta	Dell PowerEdge R620	2 x Intel Xeon CPU E5-2620 2.00 GHz	32 GB DDR3	5 x 1 TB SATA 3 x 1,2 TB SAS
Tuono	HP ProLiant DL380 G7	2 x Intel Xeon CPU E5649 2.53 GHz	32 GB DDR3	6 x 300 GB SAS 2 x 146 GB SAS
Venti	Dell PowerEdge R210 II	1 x Intel Xeon CPU E3-1220 3.10 GHz	16 GB DDR3	2 x 3 TB SATA

Tabela 4.1: Configuração dos servidores físicos.

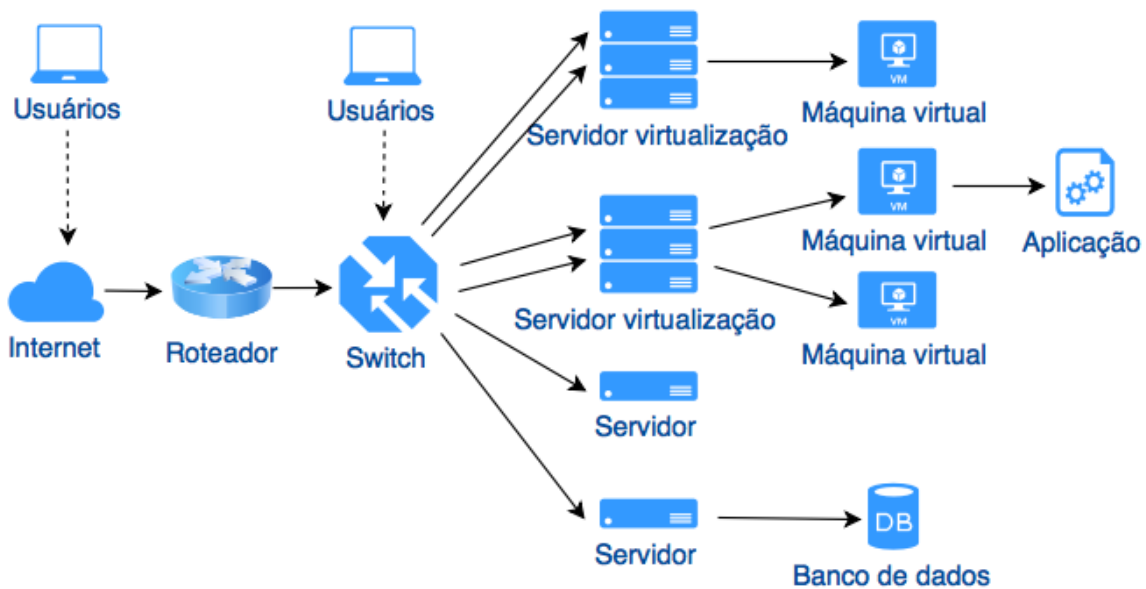


Figura 4.3: Modelo de estrutura física.

controle de versões de *software* (*Subversion (SVN) 1.8.8*), gerenciador de *bugs* (*Trac 1.0.1*), mensagens instantâneas (*Ejabberd 2.1.11*);

- Sfrunhon: outro servidor de monitoramento da rede do provedor. Esse utiliza a distribuição *CentOS 6.3* e executa a aplicação *Cacti 0.8.8a*. Esse servidor monitora atualmente o tráfego dos clientes, tanto de internet via rádio, como de fibra óptica;
- Vigilante: esse servidor é responsável por capturar e armazenar *streaming*

de vídeo de câmeras do provedor. Esse servidor possui o sistema operacional *Ubuntu 14.04 LTS*. O servidor executa a aplicação *ZoneMinder 1.29*, que também é uma ferramenta de código aberto, para capturar e armazenar as imagens das câmeras do provedor.

Os servidores de virtualização possuem suas respectivas VMs, que executam aplicações. Para virtualização utiliza-se o hipervisor KVM e a ferramenta *QEmu*, sendo que ambos são projetos de *software* livre. Procurou-se manter um ambiente homogêneo com o objetivo de facilitar a manutenção, para isso utilizou-se o mesmo hipervisor e o mesmo sistema operacional, esse sistema operacional é o sistema de código aberto *Ubuntu 14.04 LTS*. Além disso, esses servidores possuem redundância de *hardware*, com fonte de alimentação e discos configurados através de um RAID, geralmente utilizando RAID 5, em alguns casos, que possui apenas dois discos é utilizado RAID 1. O ambiente também possui uma redundância do cabeamento, como visto anteriormente.

A empresa fornece serviços diversos, desde hospedagens de sites até *Domain name system* (DNS) recursivo para o provedor de internet. Atualmente sete servidores são utilizados para virtualizar sistemas, esses servidores são os últimos sete servidores da Tabela 4.1. Sendo que existem quarenta e seis VMs distribuídas entre os sete servidores de virtualização. Para melhor entender, a seguir será descrito esses servidores e suas respectivas máquinas virtuais.

O servidor Brina possui uma VM, que executam os serviços (Figura 4.4):

- *Speedauth*: sua configuração é 2 *core* para processamento, 2?? GB de memória e 8 GB de disco. O sistema operacional é o *Ubuntu 14.04 LTS*. Esse é o servidor que fornece o serviço de autenticação *Point-to-point protocol over ethernet* (PPPoE) para maior parte dos clientes do provedor utilizando *Radius* (*Freeradius 1.??*);

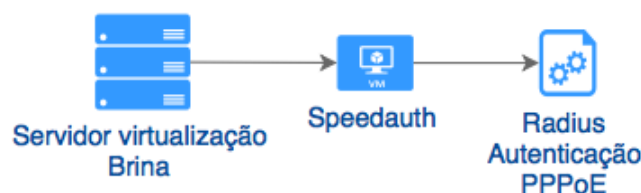


Figura 4.4: Servidor de virtualização Brina. REFAZER ???

O servidor chamado Fulmine executa onze VMs (Figura 4.5), que fornecem os seguintes serviços:

- *Servo*: sua configuração é 2 *core* para processamento, 2?? GB de memória e 20 ?? GB de disco. Esse servidor possui o sistema operacional *CentOS 6.??*. Esse servidor fornece, através do *software* ???, o serviço de DNS autoritativo e é o servidor DNS secundário dos domínios hospedados pela empresa;
- *Passata*: esse servidor possui 2?? *cores* para processamento, x?? GB de memória e 8 GB de disco. Esse servidor possui o sistema operacional *Ubuntu 14.04 LTS*. Ele fornece o serviço de DNS recursivo, através do *software BIND*??, e sendo o servidor é o primário e o mais importante para navegação dos clientes

de todo o provedor. A quantidade de requisições é ??;

- *Hotspot*: sua configuração é 1 *core* para processamento, 1?? GB de memória e 8 GB de disco. Esse servidor possui o sistema operacional *Ubuntu 14.04 LTS*. Ele é o servidor de gerência de equipamentos da *Ubiquiti* que fazem *hotspot*, que é uma tecnologia utilizada com a *Wifi* para prover acesso a internet em ambientes grandes ??, e é utilizado pelo provedor;
- *Roncon*: esse servidor possui 4 *cores* para processamento, 6?? GB de memória e 400 GB de disco. Ele possui o sistema operacional Redhat 5.?.?. Esse servidor provê acesso a sites *web* desenvolvidos com a linguagem PHP. Nele esta instalado o *software WebHost manager* (WHM), que faz a gerência dos serviços de hospedagens de sites e banco de dados. Além disso existe uma ferramenta que faz parte do WHM que é o *cPanel*, sendo que ele fornece a gerência de cada hospedagem de site para seu respectivo desenvolvedor. Para fornecer essa hospedagem os seguintes *softwares* estão instalados e configurados: *Apache 2.2*, *PHP 5.3??*, *MySQL 5.??* e *PostgreSQL 9.??*. Além da hospedagem, esse servidor fornece o serviço de autenticação ADSL de terceiros utilizando o *software Radius??*;
- *IPv6Dns*, *IPv6Dns64* e *IPv6Nat64*: suas configurações são 1 *core* para processamento, 1 GB de memória e 8 GB de disco. O sistema operacional é o *Ubuntu 14.04 LTS*. Esses servidores fornecem o serviço de DNS e *Network address translation* (NAT) para navegação *Internet protocol version 6* (IPv6) do provedor;
- *Paessler router traffic grapher* (PRTG): esse servidor possui 2 *cores* para processamento, 4?? GB de memória e 50?? GB de disco. O servidor possui o sistema operacional *Windows 2008 Server R2 ??*. Sua função é fazer o monitoramento de tráfego e equipamentos da rede *core* do provedor;
- *Masterauth*: sua configuração é 1 *core* para processamento, 1?? GB de memória e 8 GB de disco. O sistema operacional é o *Ubuntu 14.04 LTS*. Esse é o servidor que fornece o serviço de autenticação PPPoE para clientes do provedor utilizando *Radius* (*Freeradius 1.??*);
- *SimplesIP*: esse servidor possui 2 *cores* para processamento, 4?? GB de memória e 100?? GB de disco. O servidor possui o sistema operacional *CentOS 6.??*. Esse é o servidor de telefonia do provedor, que utiliza como base o *software* livre *Asterisk 2.??*;
- *Ottico*: esse servidor possui 2 *cores* para processamento, 3?? GB de memória e 50 GB de disco. O servidor possui o sistema operacional *Windows 2007 Server R??*. Ele possui o serviço de *terminal service* para suporte e gerência de fibra óptica do provedor;

O servidor chamado Piova executa oito VMs (Figura ??), que fornecem os seguintes serviços:

- *ASP*: esse servidor possui 1 *core* para processamento, 2?? GB de memória e 20?? GB de disco. O servidor possui o sistema operacional *Windows 2008 Server R2 ??*. Esse servidor provê acesso a sites *web* desenvolvidos com a linguagem *Active server pages* (ASP). Sendo que possui aproximadamente dez sites hospedados;
- *CactiBackbone*: esse servidor possui 1 *core* para processamento, 2?? GB de memória e 10?? GB de disco. Ele é um servidor de monitoramento da rede do

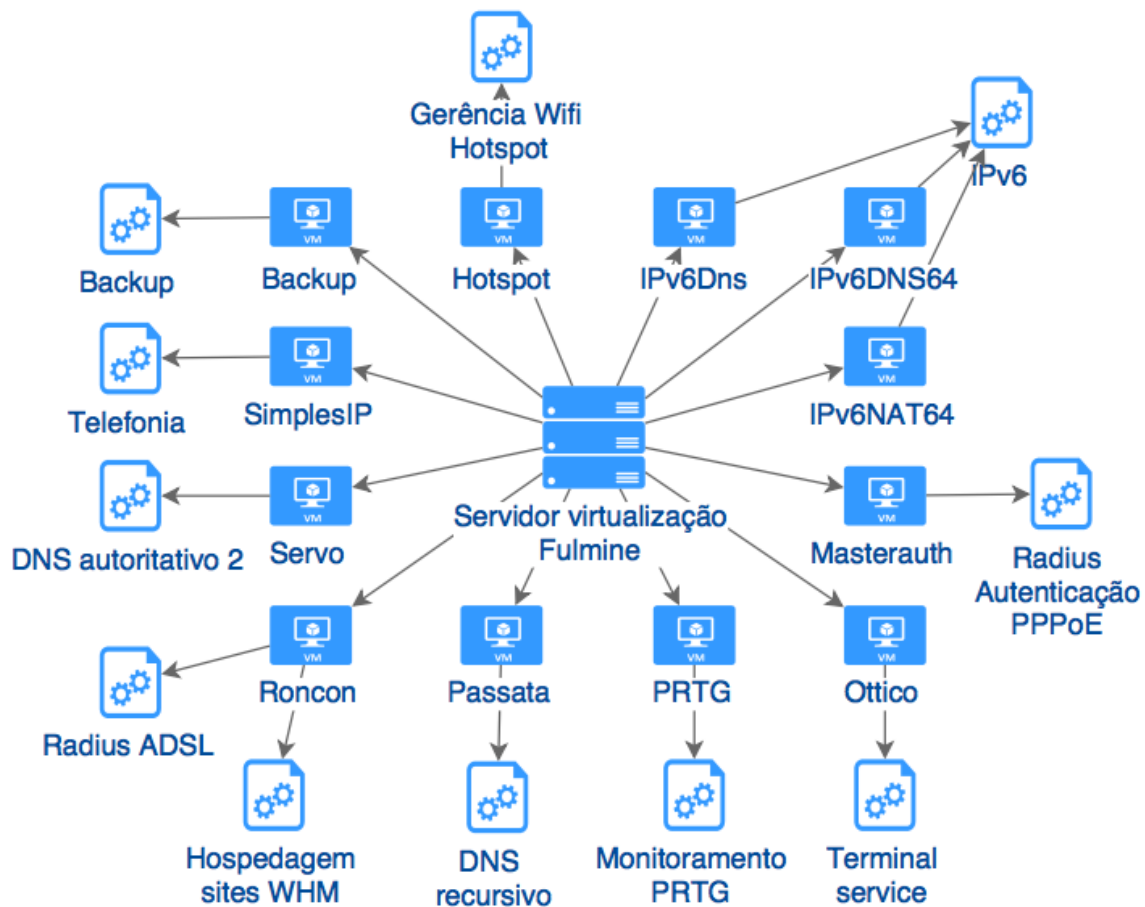


Figura 4.5: Servidor de virtualização Fulmine.

provedor. Esse utiliza a distribuição *CentOS 6.??* e executa a aplicação *Cacti 0.8.8??*. Essa aplicação monitora atualmente a uma parte da rede *backbone* do provedor;

- *Dio*: esse servidor possui 1 *core* para processamento, 1?? GB de memória e 17 GB de disco. O servidor possui o sistema operacional *Ubuntu 6.04 ??*. Esse servidor fornece serviço de hospedagens de sites desenvolvidos com a linguagem PHP versão 4, sendo que esses sites são mantidos devido a incompatibilidade com a versão 5. O número de sites é baixo, aproximadamente 10 sites;
- *FateFurbo*: sua configuração é 1 *core* para processamento, 1?? GB de memória e 8?? GB de disco. O sistema operacional é o *Ubuntu 14.04 LTS*. Ele possui um *software* proprietário que faz a gerência de uma parte da fibra óptica do provedor;
- *FiberHome*: sua configuração é 2 *core* para processamento, 2?? GB de memória e 50?? GB de disco. O sistema operacional é o *Windows XP*. Ele possui um *software* para gerência da fibra óptica do provedor;
- *Passata2*: esse servidor possui 2?? *cores* para processamento, 2?? GB de memória e 8 GB de disco. Esse servidor possui o sistema operacional *Ubuntu 14.04 LTS*. Ele fornece o serviço de DNS recursivo, através do *software BIND??*, e é o servidor secundário do provedor. A quantidade de requisições é ??;
- *Postfix*: sua configuração é 1 *core* para processamento, 1?? GB de memória e 8?? GB de disco. Esse servidor possui o sistema operacional *Ubuntu 14.04*

LTS. Esse servidor faz o envio de e-mails, através do *software Postfix x??*. Os e-mails enviados por ele são tem origem em uma ferramenta desenvolvida pela empresa, que é uma ferramenta de e-mail marketing, ou seja, faz o envio de e-mails em massa para divulgação de informações ou produtos;

- *Servo6*: sua configuração é 2 *core* para processamento, 2?? GB de memória e 20 ?? GB de disco. Esse servidor possui o sistema operacional *CentOS 6.??*. Esse servidor fornece, através do *software ???*, o serviço de DNS autoritativo e é o servidor DNS terciário dos domínios hospedados pela empresa;

O servidor chamado Raggio executa doze VMs, que fornecem os serviços de virtualização para algumas empresas. Sendo que as máquinas virtuais são instaladas com o sistema operacional da preferência do cliente, e são disponibilizadas através de um acesso remoto, como por exemplo através de *Secure shell* (SSH).

O servidor chamado Tempesta executa uma VM (Figura ??), que fornecem os seguintes serviços:

- *Merak*: esse servidor virtual fornece serviço de e-mail. Ele possui uma configuração de 6 *cores* para processamento, 10 GB de memória e 1000 GB de disco. O servidor possui o sistema operacional *Windows 2008 Server R2* e executa o *software Icewarp Server 10.4.4*. Essa aplicação fornece os serviços de envios de e-mails (*Simple mail transfer protocol* (SMTP)), recebimentos de e-mails (*Post office protocol* (POP) e *Internet message access protocol* (IMAP)), Webmail (PHP) e Anti-spam;

O servidor chamado Tuono executa oito VMs (Figura ??), que fornecem os seguintes serviços:

- *Ledriovardar*: esse servidor possui 2 *cores* para processamento, 4?? GB de memória e 50 GB de disco. O servidor possui o sistema operacional *Windows 2007 Server R2*. Ele possui o serviço de *terminal service* para suporte e gerência de fibra óptica do provedor;
- *Mondoperso*: sua configuração é 1 *core* de processamento, 1?? GB de memória e 8 GB de disco. Esse servidor possui o sistema operacional *Ubuntu 14.04 LTS*. O servidor fornece *streaming* de áudio para uma web rádio, esse serviço é feito através do *software* livre *Icecast*;
- *Monete*: sua configuração é 1 *core* de processamento, 2?? GB de memória e 50 GB de disco. Esse servidor possui o sistema operacional *Ubuntu 14.04 LTS*. Esse é um servidor *web* dedicado para o site do provedor, com configurações personalizadas. Para isso ele utiliza os *softwares Apache 2.4.7*, PHP 5.5.9 (com *PHP-FPM 5.5.9*), *MySQL 5.5.49*;
- *Ns*: esse servidor possui 2 *cores* para processamento, 4?? GB de memória e 20 GB de disco. O servidor possui o sistema operacional *CentOS 6.??*. Esse servidor fornece, através do *software ???*, o serviço de DNS autoritativo e é o servidor DNS primário dos domínios hospedados pela empresa;
- *Parla*: sua configuração é 1 *core* de processamento, 2?? GB de memória e 8 GB de disco. Ele possui o sistema operacional *Ubuntu 14.04 LTS*. Esse servidor provê um serviço de mensagens instantâneas, baseado no protocolo *Extensible messaging and presence protocol* (XMPP), para o provedor, que facilita a comunicação entre funcionários da empresa e do provedor. O *software*

utilizado é o *Ejabberd 1.??*, que também é um *software* livre;

- *Rauco*: esse servidor possui 4 *cores* para processamento, 4?? GB de memória e 300?? GB de disco. Ele possui o sistema operacional *CentOS 6.??*. Esse servidor provê acesso a sites *web* desenvolvidos com a linguagem PHP. Nele está instalado o *software* WHM, que faz a gerência dos serviços de hospedagens de sites e banco de dados. Além disso existe uma ferramenta que faz parte do WHM que é o *cPanel*, sendo que ele fornece a gerência de cada hospedagem de site para seu respectivo desenvolvedor. Para fornecer essa hospedagem os seguintes *softwares* estão instalados e configurados: *Apache 2.4*, PHP 5.6, *MySQL 5.??* e *PostgreSQL 9.??*;
- *Soldi*: sua configuração é 4 *cores* de processamento, 4 GB de memória e 40 GB de disco. Esse servidor possui o sistema operacional *Ubuntu 14.04 LTS*. Esse é um servidor *web* exclusivo para *softwares* de gestão desenvolvidos pela empresa. Os seguintes *softwares* são utilizados: *Apache 2.4.7*, PHP 5.5.9 (com *PHP-FPM 5.5.9*), *MySQL 5.5.49*;
- *Trapel*: sua configuração é 1?? *cores* de processamento, 1?? GB de memória e 8 GB de disco. Esse servidor possui o sistema operacional *Ubuntu 14.04 LTS*. Esse servidor fornece um serviço de teste de velocidade da conexão de internet, os usuários do provedor utilizam esse serviço para testar a velocidade da sua internet. Para isso ele executa uma aplicação *Apache 2.2* e um *software* desenvolvido pelo *SpeedTest (?)*;

O servidor chamado Venti executa cinco VMs (Figura ??), que fornecem os seguintes serviços:

- *Backup*: sua configuração é 1 *core* para processamento, 2 GB de memória e X?? GB de disco. Esse servidor possui o sistema operacional *Ubuntu 14.04 LTS*. Nele é executado o serviço de *backup* dos equipamentos do provedor, para isso é utilizado *scripts* que buscam e copiam os dados por *File transfer protocol* (FTP);
- *Esibire*: sua configuração é 1 *core* para processamento, 1 GB de memória e 50 GB de disco. Esse servidor possui o sistema operacional *Ubuntu 14.04 LTS*. Esse servidor faz a hospedagem de vídeos e a reprodução de *streaming*;
- *Miatanto*: sua configuração é 1 *core* de processamento, 1?? GB de memória e 8 GB de disco. Esse servidor possui o sistema operacional *Ubuntu 14.04 LTS*. O servidor fornece *streaming* de áudio para uma web rádio, esse serviço é feito através do *software* livre *Icecast*;
- *Pomodoro*: sua configuração é 1 *core* de processamento, 2?? GB de memória e 20 GB de disco. Esse servidor possui o sistema operacional *Ubuntu 14.04 LTS*. Esse servidor faz a documentação dos equipamentos do provedor, utilizando a aplicação open source? *Sakai*;
- *Quebei*: sua configuração é 1 *core* de processamento, 4?? GB de memória e 140 GB de disco. Esse servidor possui o sistema operacional *Ubuntu 14.04 LTS*. Sua função é gerenciar o *backup* dos outros servidores, para isso ele utiliza a ferramenta *Bacula 5.2.6* (pacote *bacula-director-common 5.2.6*). Além disso, esse servidor possui o sistema gerenciador de banco de dados *MySQL 5.??* instalado, que está configurado como *master-slave*, sendo que esse servidor é o *slave* e o servidor *Dati* é o *master*;

-graficos cpu memoria disco cada servidor de virtualizacao?? colocar aqui ou na implementacao??

-citar ferramentas monitoramento, gerenciamento, update e backup??

4.2 Serviços críticos

Na seção anterior foram detalhados todos os serviços que estão atualmente disponíveis na empresa, com isso nesta seção será feita a identificação dos serviços mais críticos para a empresa.

Para selecionar os serviços críticos anteriormente foram detalhados todos os serviços. Sendo assim os seguintes critérios serão utilizados para selecionar os serviços mais críticos, assim possibilitando a implementação do ambiente de alta disponibilidade:

- A quantidade de clientes ou funcionários que utilizam o serviço: esse é o item mais relevante, pois impacta diretamente no faturamento da empresa. Por exemplo, se um cliente ficar sem acesso à internet, a sua mensalidade pode ser reduzida de acordo com o tempo que ele ficou sem acesso;
- O número de requisições em um determinado tempo: esse número é importante, devido ao fato de indicar ações dos usuários. Sabe-se que quanto mais ações, mais usuários dependem do serviço. São exemplos dessa medida: quantidade de acessos por minuto em um servidor de hospedagens de sites, ou quantidade de requisições DNS a um servidor recursivo;
- O volume de objetos do serviço: essa medida demonstra a abrangência do serviço, ou seja, qual a demanda que o serviço pode atingir. Por exemplo, a quantidade de equipamentos monitorados por um servidor de monitoramento.

Deste modo, pode-se afirmar que esses critérios são importantes, pois caso os serviços relacionados a eles fiquem indisponíveis causarão um prejuízo financeiro para a empresa.

Os serviços mais críticos estão listados a seguir e ordenados de acordo com sua relevância:

- DNS recursivo primário: esse serviço foi classificado como mais importante pois possui um impacto direto nos clientes do provedor, e é o único serviço que todos os clientes utilizam, que totalizam aproximadamente 9000 clientes. Sendo um provedor de internet, sua prioridade é fornecer uma navegação de qualidade aos seus clientes, sabendo que o DNS é fundamental para essa navegação, assim caracterizando essa importante classificação. Outro importante critério é o número de requisições por segundo (Figura GRAFICO??), que é o maior entre todos os outros serviços;
- *Radius*: esse serviço também é importante para navegação dos clientes do provedor, pois, como visto anteriormente, ele faz a autenticação dos clientes de acesso a internet de todo o provedor, que chega aproximadamente da 9000 clientes. Caso esse serviço fique indisponível os clientes não conseguirão estabelecer conexão para navegar, sabendo que atualmente esse serviço recebe x?? requisições de autenticação por x (Figura GRAFICO FREERADIUS??). Além disso, esse serviço armazena dados de clientes como: o endereço de *Internet protocol* (IP) de cada cliente utilizado em um determinado período, o

tráfego de dados da conexão, o tempo da conexão de cada cliente, entre outros. Essas operações resultam em um número de requisições por segundo, que está detalhado na Figura GRAFICO??;

- **Sistemas:** esse serviço não tem um grande impacto direto para os clientes, porém tem um grande impacto para os funcionários da empresa e do provedor. Totalizando x?? funcionários, caso houver uma indisponibilidade dos sistemas a maior parte desses funcionários ficarão impossibilitados de trabalhar (aproximadamente x?? funcionários simultâneos de acordo com a Figura GRAFICO??), isso poderia gerar um prejuízo elevado para a empresa e o provedor. Sendo que o sistema do provedor é responsável pela maior parte das operações do provedor, como por exemplo, emissão de boletos e envio para clientes, atendimento de clientes, comunicação interna da empresa, vendas, ativações de novos clientes, entre outros;
- **Telefonia:** esse serviço tem relevância para a empresa e para o provedor, pois permite a comunicação entre clientes e funcionários, e também entre funcionários e outros funcionários, sendo essencial para qualquer empresa. Sabendo que possui uma média de x?? ligações por xx (Figura GRAFICO??), sendo que essas ligações são utilizadas por todos os setores do provedor e também da empresa. Exemplos práticos são: atendimento a clientes para suporte técnico, comunicação interna entre funcionários, cobranças a clientes inadimplentes, ??... Levando isso em consideração, se esse serviço ficar indisponível irá gerar prejuízos para a empresa.

Tendo esses serviços pode-se identificar quais máquinas virtuais serão incluídas no ambiente de alta disponibilidade, que são:

- *Passata*
- *Speedauth*
- *Masterauth*
- *Soldi*
- *SimplesIP*

Os recursos virtuais somados são 11 *cores* de processamento, 12 GB de memória e 156 GB de disco.

-Exibir disponibilidade média atual dos serviços, com gráficos??

5 PROPOSTA DE SOLUÇÃO

REFERÊNCIAS

ANDRADE, L. **Visão geral sobre virtualização**. <Disponível em: <https://tecnologiasemsegredos.wordpress.com/category/virtualizacao/>>. Acesso em 21 de maio de 2016.

BATISTA, A. C. **Estudo teórico sobre cluster linux**. 2007. Pós-Graduação(Administração em Redes Linux) — Universidade Federal de Lavras, Minas Gerais.

BUYYA, R.; VECCHIOLA, C.; SELVI, S. **Mastering Cloud Computing: foundations and applications programming**. [S.l.]: Elsevier, 2013.

CARISSIMI, A. Virtualização: da teoria a soluções. In: **Minicursos do Simpósio Brasileiro de Redes de Computadores**. Porto Alegre: XXVI Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos, 2008.

Citrix. **The Xen Project, the powerful open source industry standard for virtualization**. <Disponível em: <http://www.xenproject.org/>>. Acesso em 22 de maio de 2016.

Citrix. **XenApp and XenDesktop - Virtual Apps and Desktops**. <Disponível em: <https://www.citrix.com/products/xenapp-xendesktop/>>. Acesso em 22 de maio de 2016.

COSTA, H. L. A. **Alta disponibilidade e balanceamento de carga para melhoria de sistemas computacionais críticos usando software livre: um estudo de caso**. 2009. Pós-Graduação em Ciência da Computação — Universidade Federal de Viçosa, Minas Gerais.

GONÇALVES, E. M. **Implementação de Alta disponibilidade em máquinas virtuais utilizando Software Livre**. 2009. Trabalho de Conclusão (Curso de Engenharia da Computação) — Faculdade de Tecnologia e Ciências Sociais Aplicadas, Brasília.

IBM. **System/370 Model 145**. <Disponível em: https://www-03.ibm.com/ibm/history/exhibits/mainframe/mainframe_PP3145.html>. Acesso em 22 de maio de 2016.

LAUREANO, M. A. P.; MAZIERO, C. A. Virtualização: conceitos e aplicações em segurança. In: **Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais**. Gramado - Rio Grande do Sul: VIII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais, 2008.

MARINESCU, D. **Cloud Computing**: theory and practice. [S.l.]: Elsevier Science, 2013.

MAZIERO, C. A. **Sistemas Operacionais**: conceitos e mecanismos. 2013. Dissertação (Mestrado em Ciência da Computação) — DAIInf UTFPR, Paraná.

MOREIRA, D. **Virtualização**: rode vários sistemas operacionais na mesma máquina. <Disponível em: <http://idgnow.com.br/ti-corporativa/2006/08/01/idgnoticia.2006-07-31.7918579158/#&panel1-3>>. Acesso em 5 de abril de 2016.

NØRVÅG, K. **An Introduction to Fault-Tolerant Systems**. 2000. IDI Technical Report 6/99 — Norwegian University of Science and Technology, Trondheim, Noruega.

Oracle. **Oracle VM VirtualBox**. <Disponível em: <https://www.virtualbox.org/>>. Acesso em 22 de maio de 2016.

PANKAJ, J. **Fault tolerance in distributed system**. Nova Jérsei, Estados Unidos: P T R Prentice Hall, 1994.

PEREIRA FILHO, N. A. **Serviço de pertinência para clusters de alta disponibilidade**. 2004. Dissertação para Mestrado em Ciência da Computação — Universidade de São Paulo, São Paulo.

QEmu. **QEMU open source processor emulator**. <Disponível em: http://wiki.qemu.org/Main_Page>. Acesso em 22 de maio de 2016.

REIS, W. S. dos. **Virtualização de serviços baseado em contêineres**: uma proposta para alta disponibilidade de serviços em redes linux de pequeno porte. 2009. Monografia Pós-Graduação(Administração em Redes Linux) — Apresentada ao Departamento de Ciência da Computação, Minas Gerais.

ROUSE, M. **Hot spare**. <Disponível em: <http://searchstorage.techtarget.com/definition/hot-spare>>. Acesso em 12 de abril de 2016.

SILVA VIANA, A. L. da. **MySQL**: replicação de dados. <Disponível em: <http://www.devmedia.com.br/mysql-replicacao-de-dados/22923>>. Acesso em 21 de abril de 2016.

SILVA, Y. F. da. **Uma Avaliação sobre a Viabilidade do Uso de Técnicas de Virtualização em Ambientes de Alto Desempenho**. 2009. Trabalho de Conclusão (Curso de Ciência da Computação) — Universidade de Caxias do Sul, Caxias do Sul - Rio Grande do Sul.

SMITH, J. E.; NAIR, R. The architecture of virtual machines. **IEEE Computer**, [S.l.], v.38, p.32–38, 2005.

SMITH, R. **Gerenciamento de Nível de Serviço**. <Disponível em: <http://blogs.technet.com/b/ronaldosjr/archive/2010/05/25/gerenciamento-de-n-237-vel-de-servi-231-o.aspx>>. Acesso em 25 de março de 2016.

VMware. **VMware ESXi**. <Disponível em: <http://www.vmware.com/products/esxi-and-esx/overview.html>>. Acesso em 22 de maio de 2016.

VMware. **VMware Workstation Player (formerly known as Player Pro)**. <Disponível em: <https://www.vmware.com/products/player>>. Acesso em 22 de maio de 2016.

VMware. **VDI Virtual Desktop Infrastructure with Horizon**. <Disponível em: <https://www.vmware.com/products/horizon-view>>. Acesso em 22 de maio de 2016.

WEBER, T. S. **Um roteiro para exploração dos conceitos básicos de tolerância a falhas**. 2002. Curso de Especialização em Redes e Sistemas Distribuídos — UFRGS, Rio Grande do Sul.

WineHQ. **WineHQ - Execute aplicativos Windows no Linux, BSD, Solaris e Mac OS X**. <Disponível em: <https://www.winehq.org/>>. Acesso em 22 de maio de 2016.

VMware. **VMware Workstation Pro**. <Disponível em: <http://www.vmware.com/br/products/workstation>>. Acesso em 17 de maio de 2016.