

UNIVERSIDADE FEDERAL DO ESTADO DO RIO DE JANEIRO – UNIRIO

DAVI SCHIAVINI JARDIM

VIRTUALIZAÇÃO DE SERVIÇOS DE REDE NO IFRJ

RIO DE JANEIRO

2014

DAVI SCHIAVINI JARDIM

VIRTUALIZAÇÃO DE SERVIÇOS DE REDE NO IFRJ

Trabalho de Conclusão de Curso apresentado à Universidade Federal do Estado do Rio de Janeiro, como requisito para a conclusão do curso de Bacharelado em Sistemas de Informação.

Orientador: Professor Sidney Cunha de Lucena

RIO DE JANEIRO

2014

DAVI SCHIAVINI JARDIM

VIRTUALIZAÇÃO DE SERVIÇOS DE REDE NO IFRJ

Trabalho de Conclusão de Curso apresentado à Universidade Federal do Estado do Rio de Janeiro, como requisito para a conclusão do curso de Bacharelado em Sistemas de Informação.

Aprovada em 2014

Banca Examinadora

Prof. Leonardo Luiz Alencastro Rocha

UNIRIO

Prof. Morganna Carmem Diniz

UNIRIO

Prof. Sidney Cunha de Lucena

UNIRIO

Dedico este projeto a Deus, à
minha noiva, e aos familiares,
que me apoiaram sempre, me
entenderam, e em nenhum
momento desistiram de mim
durante todo esse longo
caminho.

AGRADECIMENTOS

Louvo o meu Deus, soberano sobre tudo e todos. Dou graças a Ele por tudo que tem feito por mim. Por me trazer desde o nada, e conduzir minha vida com paciência, misericórdia, graça e autoridade até onde estou. Ao Senhor e Salvador da minha vida, tudo que sou e tudo que tenho.

À Universidade Federal do Estado do Rio de Janeiro, e pelo corpo de professores da Escola de Informática Aplicada por ter me acolhido em seu espaço para me educar e me dar essa oportunidade ímpar de aprendizado e crescimento.

Ao Professor Sidney, meu orientador, por ter recebido tão bem minha proposta e ter se dedicado a me orientar ao longo de toda a construção deste trabalho. Suas contribuições foram fundamentais e valiosas.

À minha família por ter me suportado e me apoiado nesses anos de estudo, ajudando como podiam.

À minha noiva, minha musa, presente de Deus na minha vida, que me inspira a crescer mais e aprender mais a cada dia. Sua ajuda e incentivo foram essenciais para conclusão deste trabalho. Sem ela, eu não teria conseguido. Sem ela, eu não teria conseguido.

A todos que direta ou indiretamente fizeram parte da minha formação, meus mais sinceros agradecimentos.

RESUMO

A presente monografia trata da virtualização de serviços dentro do ambiente de rede do Instituto Federal de Educação, Ciência e Tecnologia do Rio de Janeiro. Neste trabalho, verifica-se o rápido e amplo crescimento do Instituto, suas demandas técnicas, e as características anteriores à implantação do projeto. Logo após, são discutidas soluções correntes para virtualização com algumas características específicas, como alta disponibilidade e migração de máquinas virtuais sem reinício. Em seguida, descreve-se brevemente as infraestruturas anterior e a implementada no IFRJ, para enfim, demonstrar o funcionamento da arquitetura implementada, mostrando suas aplicações práticas, e identificando limitações de sistema, assim como pontos de possíveis melhorias futuras. Por último, conclui-se o trabalho com observações sobre as etapas do trabalho e considerações sobre o futuro da solução.

Palavras chave:

Virtualização, serviços, rede, interligação, datacenter.

ABSTRACT

This monograph comes to the virtualization services within the network environment of the Federal Institute for Education, Science and Technology of Rio de Janeiro. In this work, the rapid and extensive growth of the Institute is contemplated, as well as its technical demands and characteristics prior to project implementation. Soon after, current virtualization solutions are discussed, along with some specific features such as high availability and live migration of virtual machines without restarting. Then, the previous infrastructure implemented in IFRJ is briefly discussed, in order to show how the architecture was implemented, explaining its practical applications, and identifying system limitations, as well as points of possible future improvements. Finally, this monograph concludes with observations on the progress of the work and considerations about the future of the solution.

Hint words:

Virtualization, services, network interconnection, datacenter.

LISTA DE IMAGENS

Figura 1 - Hipervisor tipo 1	28
Figura 2 - Hipervisor tipo 2	29
Figura 3 - Topologia de interligação dos campi	33
Figura 4 - Topologia de funcionamento da rede do datacenter	35
Figura 5 - Exemplo de desempenho das conexões à Internet no Instituto	36
Figura 6 - Teste de conexão entre dois campi	38
Figura 7 - Hospedeiros antes da migração.....	39
Figura 8 - Hospedeiros depois da migração	39
Figura 9 - Exemplo de desempenho das interconexões no Instituto	44

LISTA DE TABELAS

Tabela 1 - Proporção de empresas que ofereceram acesso remoto.	12
Tabela 2 – Endereçamento utilizado no Instituto, por campus	30

LISTA DE ABREVIATURAS E SIGLAS

ADSL Asymmetric Digital Subscriber Line

AP Access Point

ATA Advanced Technology Attachment

CEFETEQ Centro Federal de Educação Tecnológica de Química

CETIC Centro de Estudos sobre as Tecnologias da Informação e da Comunicação

CPU Central Processing Unit

DHCP Dynamic Host Configuration Protocol

DNS Domain Name Server

HD Hard Drive

IFRJ Instituto Federal de Educação, Ciência e Tecnologia do Rio de Janeiro

IP Internet Protocol

MPLS Multipacket Label Switching

PCI Peripheral Component Interconnect

RAID Redundant Array of Independent Drives

RAM Random Access Memory

RNP Rede Nacional de Pesquisas

SAN Storage Area Network

SAS Serial Attached SCSI

SATA Serial ATA

SIGA-ADM Sistema Integrado de Gestão Administrativa – Módulo Administrativo

SIGA-EDU Sistema Integrado de Gestão Administrativa – Módulo Educacional

SCSI Small Computer System Interface

TI Tecnologia da Informação

USB Universal Serial Bus

VM Virtual Machine

VoIP Voice over IP

VPN Virtual Private Network

SUMÁRIO

1. INTRODUÇÃO	12
1.1. Motivação	13
1.2. Objetivo Geral	14
1.3. Objetivo Específico	14
1.4. Metodologia.....	14
1.5. Organização	15
2. PANORAMA DE TI DO IFRJ.....	16
2.1. Campi.....	16
2.2. Datacenters	16
2.3. Infraestrutura de Rede.....	17
2.4. Usuários	17
3. SERVIÇOS A SEREM DISPONIBILIZADOS.....	18
3.1. Serviço de diretório.....	18
3.2. Compartilhamento de arquivos.....	18
3.3. Compartilhamento de impressoras	19
3.4. Virtualização de aplicativos.....	19
3.5. Virtualização de máquinas Windows/Linux.....	19
3.6. Ambientes de produção/desenvolvimento	20
3.7. Não-interrupção de serviços	20
3.7.1. Minimizando falhas de conexão de dados	21
3.7.2. Minimizando falhas de infraestrutura.....	21
4. SOLUÇÃO DE DATACENTER BASEADO EM VIRTUALIZAÇÃO.....	22
4.1. Virtualização.....	22
4.2. Soluções para alta disponibilidade.....	23
4.2.1. Tolerância a falhas	23
4.3. Balanceamento de carga	24
4.4. Migração de VMs sem reinício.....	24
4.5. Outras opções.....	24
4.6. Soluções disponíveis.....	25
5. ARQUITETURA IMPLEMENTADA NO IFRJ.....	26
5.1. Arquitetura anterior	26
5.1.1. Infraestrutura de rede	26

5.1.2.	Virtualização.....	27
5.1.3.	Serviços.....	27
5.2.	Soluções escolhidas	28
5.2.1.	Virtualização.....	28
5.2.2.	Infraestrutura de Rede.....	30
5.3.	Ambiente implementado.....	32
5.3.1.	Infraestrutura de Rede.....	32
5.3.2.	Sistema de Virtualização	34
5.3.3.	Serviços.....	35
6.	FUNCIONAMENTO DA ARQUITETURA IMPLEMENTADA.....	36
6.1.	Resultado de implementação	36
6.2.	Balanceamento de carga	38
6.3.	Usuários	40
6.4.	Limitações de sistema.....	40
6.5.	Políticas de segurança.....	41
6.6.	Receptividade dos usuários à nova infraestrutura	42
6.7.	Desempenho geral do sistema	43
6.8.	Futuros objetos de melhoria.....	44
7.	CONCLUSÃO.....	46
8.	REFERÊNCIAS	48

1. INTRODUÇÃO

O Instituto Federal de Educação, Ciência e Tecnologia do Rio de Janeiro - IFRJ foi criado em 29 de dezembro de 2008, em resolução a Lei 11.892. Suas estruturas foram incorporadas do Centro Federal de Educação Tecnológica de Química - CEFETEQ. O principal foco do IFRJ é a formação de jovens e adultos seguindo os conceitos éticos do desenvolvimento sustentável.

O IFRJ consolidou-se como referência nacional em educação científica e tecnológica através de cursos integrados ao ensino médio, em concomitância com o ensino médio, graduação e pós graduação lato/stricto sensu. Em suas onze unidades de ensino, são oferecidos cursos como: técnico em eletrotécnica, técnico em metrologia, licenciatura em física e bacharelado em ciências biológicas.

Tabela 1 - Proporção de empresas que ofereceram acesso remoto.

Percentual (%)		E-mail corporativo	Sistema de computadores da empresa	Pastas e arquivos da empresa
TOTAL		57	56	49
PORTE	De 10 a 49 pessoas ocupadas	52	52	45
	De 50 a 249 pessoas ocupadas	73	69	61
	De 250 ou mais pessoas ocupadas	85	81	73
REGIÃO	Norte	54	57	51
	Nordeste	55	61	52
	Sudeste	59	54	49
	Sul	55	56	49
	Centro-Oeste	58	59	53
MERCADOS DE ATUAÇÃO - CNAE 2.0	Indústria de transformação	59	50	50
	Construção	63	53	51
	Comércio; reparação de veículos automotores e motocicletas	55	59	48
	Transporte, armazenagem e correio	61	58	57
	Alojamento e alimentação	38	46	31
	Atividades imobiliárias; atividades profissionais, científicas e técnicas; atividades administrativas e serviços complementares.	66	62	61
	Informação e comunicação	80	71	65
	Artes, cultura, esporte e recreação; outras atividades de serviços	61	59	52

O uso da Internet em empresas, escolas e domicílios aumenta significativamente a cada dia. Com a facilidade do acesso e compartilhamento pela rede, milhões de pessoas trocam informações em poucos segundos. A área de Tecnologia da Informação em

empresas cresce igualmente. A Tabela 1 apresenta uma pesquisa divulgada pela CETIC¹, onde observa-se a proporção de empresas que disponibiliza acesso remoto a seus serviços.

Atualmente, a estrutura de Tecnologia da Informação do IFRJ funciona em dois datacenters, localizados em duas unidades diferentes. Seu datacenter principal possui uma estrutura de “produção-contingência”, e sistema de cópia de segurança através de fita magnética.

O projeto que será descrito a seguir explicita os procedimentos executados para a virtualização dos servidores do IFRJ.

1.1. Motivação

Devido ao crescimento extremamente rápido e substancial do Instituto, viu-se a necessidade de expandir o parque de sistemas informatizados, bem como paramentar o mesmo de tecnologia necessária para integração dos dados dos campi, facilitar os processos comunicativos entre as unidades, providenciar infraestrutura gerenciável de TI, estabelecer meios de garantia de segurança da informação, e unificar e homogeneizar toda a estrutura que envolve os sistemas de informação atualmente em funcionamento na instituição.

A criação do Instituto Federal do Rio de Janeiro a partir da antiga Escola Técnica Federal de Química juntou os campi desta (a saber: campus Rio de Janeiro e campus Nilópolis), com diversas unidades provenientes de outras instituições de ensino, como por exemplo, o campus agrícola Nilo Peçanha, e outras unidades criadas após a fundação do IFRJ, como por exemplo, o campus Mesquita.

Dada essa rápida expansão, a Diretoria de Gestão de Tecnologia da Informação se viu com o desafio de criar uma plataforma única, homogênea, centralizada, com ambiente de rede comum a todos os usuários, que interconectasse os campi, facilitasse a troca de dados, e favorecesse a segurança da informação e a gerência dos serviços oferecidos.

¹ Base: 6.225 empresas que declararam utilizar computador com 10 ou mais pessoas ocupadas e que constituem os seguintes segmentos da CNAE 2.0 (C, F, G, H, I, J, L, M, N, R e S) Fonte: <http://www.cetic.br/tics/empresas/2013/geral/A4C/>

1.2. Objetivo Geral

Este trabalho tem como objetivo especificar cada conceito da infraestrutura de computação e da infraestrutura de rede existentes, e sua sincronia para o desenvolvimento e implementação do projeto proposto.

Destacam-se os seguintes tópicos entre os objetivos do projeto:

- Padrões existentes no IFRJ;
- Soluções disponíveis;
- Desenvolvimento e implantação dos padrões em concomitância com a estrutura projetada;

1.3. Objetivo Específico

Com vista nos objetivos motivacionais citados anteriormente, optou-se por uma estrutura de TI centralizada em um datacenter, onde seriam hospedados e gerenciados todos os serviços comuns a toda a instituição. Considerando, também, que há muitos serviços em funcionamento, que são necessárias plataformas de testes e treinamento para cada um dos serviços em funcionamento, e a possível expansão dos serviços de TI no futuro, a equipe de TI decidiu utilizar extensivamente a solução de virtualização do ambiente de servidores, utilizando um hardware robusto e um sistema de virtualização com suporte a diversas funcionalidades consideradas essenciais, tais como remanejamento de máquinas virtuais sem reinício, alta disponibilidade, compartilhamento de *storage* entre os diferentes *hosts* de virtualização.

1.4. Metodologia

A metodologia utilizada neste projeto foi o estudo de todas as tecnologias disponíveis e os resultados desejados. Desta forma, foi definida uma lista de etapas necessárias para o desenvolvimento do projeto, elas são:

- I. Análise de tecnologias disponíveis no IFRJ;
- II. Pesquisa de soluções disponíveis para implementação do projeto;
- III. Procedimento comparativo e definição da solução adequada;
- IV. Desenvolvimento e implementação da solução;

V. Observação do desempenho do projeto e definição de melhorias futuras;

1.5. Organização

A pesquisa apresentada foi estruturada em oito capítulos.

O primeiro capítulo trata dos objetivos e motivações para a implementação deste projeto. O capítulo 2 possui todo o panorama do IFRJ e sua estrutura. No capítulo 3 serão evidenciados os serviços a serem oferecidos, a virtualização e o ambiente de desenvolvimento e implantação. O capítulo 4 expõe as soluções disponíveis para alta disponibilidade e balanceamento. No capítulo 5 temos a apresentação da arquitetura disponível no IFRJ juntamente com o ambiente implementado. O capítulo 6 demonstra o funcionamento e desempenho do projeto, e seus objetos de melhoria. No capítulo 7 foi descrita uma conclusão de todo o trabalho. O capítulo 8 encerra esta pesquisa, explicitando as referências utilizadas para sua construção.

2. PANORAMA DE TI DO IFRJ

Para entender o ambiente onde o projeto será executado, é necessário visualizar um panorama geral do IFRJ, contemplando as pessoas que compõem o sistema, o ambiente tecnológico existente e as necessidades correntes.

2.1. Campi

No momento da execução deste trabalho, o IFRJ possuía onze campi. São eles: Arraial do Cabo, Duque de Caxias, Engenheiro Paulo de Frontin, Mesquita, Nilópolis, Paracambi, Pinheiral, Realengo, Rio de Janeiro, São Gonçalo e Volta Redonda. Além destes, o IFRJ possui uma Reitoria, uma unidade puramente administrativa, que está localizada no Rio de Janeiro. Todos os campi possuem coordenações especializadas em tecnologia da informação, mas todos os serviços que envolvam servidores e seus serviços são desenvolvidos na reitoria.

Cada campi tem sua estrutura de datacenter própria, inicialmente gerenciada pela sua coordenação de suporte de TI. Esse parque de servidores particulares de cada campus contempla diferentes tecnologias, embora utilizem as mesmas máquinas para hospedar os sistemas operacionais servidores. Cada campus tem focos diferentes de ensino, o que se reflete na infraestrutura de TI disponível à época de execução do projeto, assim como a utilização dessa estrutura.

Os campi têm autonomia sobre sua infraestrutura de TI. Administrativamente, as coordenações de suporte de TI de cada campus não possuem ligação direta com a reitoria, embora haja uma relação de cooperação estável e de bons relacionamentos entre as unidades, incluindo a reitoria.

2.2. Datacenters

O IFRJ possui dois datacenters. O principal localizado no campus Rio de Janeiro, e um datacenter de contingência localizado na Reitoria.

Todos os campi do IFRJ e os serviços de TI utilizados neles são concentrados em servidores do datacenter principal. O datacenter possui uma estrutura de produção-congênita, com backup em fita magnética. O projeto de virtualização de servidores foi implementado neste datacenter.

Apesar disso, cada campus tem um par de servidores Dell com sistema de virtualização para hospedagem de servidores para serviço da rede interna do campus. Isto é feito para serviços de acesso local, como acesso ao diretório de usuários, compartilhamento de arquivos específico do campus, servidor de impressão, entre outros.

2.3. Infraestrutura de Rede

A infraestrutura de rede era gerenciada individualmente por cada campus. Não existia, anteriormente ao projeto, nenhum padrão de topologia e, portanto, cada setor de suporte de cada campus resolvia suas dificuldades do jeito que melhor lhes cabia. Isso incluía cabeamento e rede sem fio.

O cabeamento era, frequentemente, estendido com o uso de switches domésticos, e o risco de surgimento de loops na rede era alto, ocasionando paradas na rede por causa da sobrecarga originária do loop. Também não havia discriminação quanto aos dispositivos que se conectavam na rede cabeada. Adicionalmente, o uso destes switches implica em pontos de convergência da rede não gerenciáveis, e portanto, passíveis de se tornarem pontos de falha de segurança de rede.

A rede sem fio era inexistente em alguns campi, e em outros era feita usando equipamentos domésticos configurados de acordo. Não havia um critério específico, apenas soluções localizadas para problemas específicos.

2.4. Usuários

Entre os usuários dos sistemas de informação do Instituto encontram-se técnicos administrativos, professores e estagiários, sendo este último grupo o menos expressivo quantitativamente.

Professores têm pouco uso dos sistemas, exceto os que envolvem digitação de notas e registro de frequências. A exceção à regra são os professores que ocupam cargos administrativos, onde precisam fazer acesso regular aos sistemas da instituição, e por isso acabam por fazer um uso mais intensivo dos recursos disponíveis. Técnicos administrativos são os usuários mais intensos dos recursos de TI fornecidos. Estão a todo momento utilizando o armazenamento em rede, acessam os mais variados tipos de sistemas, internos e externos ao Instituto, e fornecem apoio logístico e administrativo a todas as atividades desenvolvidas em sala de aula e fora dela.

3. SERVIÇOS A SEREM DISPONIBILIZADOS

Para projetar corretamente o novo ambiente de processamento de dados do Instituto, é preciso entender alguns dos serviços que são oferecidos hoje, para compreender as demandas do novo ambiente.

3.1. Serviço de diretório

Este serviço representa o gerenciamento e a organização de todas as contas de usuário, e associações de computadores e servidores, em uma estrutura baseada em domínio. Neste serviço, há a possibilidade de se agrupar entidades do domínio em grupos e/ou unidades organizacionais, facilitando a organização dos ativos do domínio e a aplicação de configurações para todos, ou para grupos específicos.

Este serviço é essencial, pois contendo todas as contas de usuário do domínio, estes só poderão acessar as estações de trabalho e utilizar os recursos de rede após terem seus registros no serviço. Isto significa identificação de todos os indivíduos que fazem acesso aos recursos de trabalho, seja hardware ou software, em ambiente particular ou compartilhado. Caso seja necessário auditoria ou investigação, a identificação dos responsáveis por determinadas ações é fundamental, e o serviço de diretório permite esse registro.

Um diretório que englobe todas as contas de usuários e represente a estrutura organizacional interna do Instituto também traz benefícios externos, como a possibilidade de integração com aplicações que suportem LDAP, ou que possam ser diretamente integradas ao Active Directory da Microsoft. Essa integração é particularmente útil quando se deseja implantar um serviço para todos na instituição, mas que necessite de autenticação e identificação dos usuários.

3.2. Compartilhamento de arquivos

Erros em estações de trabalho são comuns, e o risco de um erro desses causar danos irreparáveis ao sistema operacional expõe, automaticamente, os usuários a riscos de perda de dados armazenados na estação. Aliado a isso, sempre existe o risco de se criar duplicatas de arquivos conforme eles são enviados e reenviados entre os funcionários para trabalhos coletivos. Isso pode criar confusões sobre versão de arquivos, e pode também

gerar problemas de espaço, já que as duplicatas vão tomando espaço em disco desnecessário nos locais onde estão armazenadas.

Pensando nisso, foi oferecido, desde antes, o serviço de compartilhamento de arquivos. Neste serviço, cada grupo de usuários tem direito a uma pasta comum, privativa ao grupo, com 5GB de espaço, e cada usuário tem direito a uma pasta privativa com 100MB de espaço. Isto é para que arquivos pessoais, e arquivos comuns a um grupo de pessoas, sejam armazenados em um servidor na rede, para evitar perdas de dados nos clientes, e facilitar a recuperação de dados através do backup de um único ponto.

3.3. Compartilhamento de impressoras

Em um ambiente empresarial, uma mesma impressora é utilizada por vários funcionários. Para gerenciar este uso, foi oferecido, em conjunto com o diretório e o compartilhamento de arquivos, o serviço de compartilhamento de impressoras, a fim de que todos possam utilizar as impressoras comuns.

Uma utilidade adicional do serviço, é o gerenciamento de impressoras de grupo. Uma impressora pertencente a um determinado departamento ou setor só pode ser utilizada pelos funcionários de lá. Outros funcionários só poderão utilizar caso o setor de domicílio da impressora autorizar.

3.4. Virtualização de aplicativos

A virtualização pode ser definida como um ambiente ou plataforma virtual para o armazenamento de recursos, instalação de diversos sistemas e execução de múltiplos serviços. É basicamente uma camada física e diversas camadas lógicas. A virtualização de aplicações transforma aplicativos em serviços virtuais gerenciáveis, de forma que não afetem o funcionamento de outros aplicativos, ou seja, o aplicativo fica encapsulado em uma máquina virtual.

Algumas das vantagens da virtualização de aplicativos são: mais segurança no sistema operacional, economia na manutenção e suporte de máquinas.

3.5. Virtualização de máquinas Windows/Linux

A virtualização de desktops foi concebida como uma alternativa aos elevados custos de implantação e manutenção de estações de trabalho completas para empresas. A

virtualização de uma estação de trabalho envolve um hardware com poder de processamento e memória suficientes para executar diversas sessões de usuários, e a implantação de “thin clients”, ou “clientes finos”, ou ainda “clientes burros”, que serão responsáveis apenas por conectar o usuário ao hardware central, e prover as entradas de mouse e teclado, a saída de vídeo, e as interfaces de mão dupla para outras conexões como áudio, USB e outras.

Estes clientes finos não terão nenhuma carga de processamento ou execução além das funções básicas de conectar ao hardware central. Facilitam a manutenção, pois toda a administração e manutenção do sistema operacional e dos aplicativos são feitas no servidor de virtualização, e os problemas originários no hardware do cliente são restritos ao funcionamento do cliente fino, que é altamente simples.

3.6. Ambientes de produção/desenvolvimento

Os serviços oferecidos, em sua maior parte, têm seu código fonte alterado por uma equipe de programadores residentes que, eventualmente, precisam de um ambiente de desenvolvimento e teste para evitar que alterações com erros sejam publicadas nos servidores de produção.

Para este fim, é necessário que haja recursos suficientes para a execução de máquinas de desenvolvimento, particularmente a possibilidade de usar snapshots nas máquinas virtuais de desenvolvimento, para teste e recuperação rápidos.

3.7. Não-interrupção de serviços

É de extrema importância que os serviços disponibilizados não sejam interrompidos por quaisquer motivos. Possíveis interrupções podem originar de falhas de equipamentos de rede, falhas em serviços de conexão contratados, falhas na execução dos servidores, falhas na infraestrutura de suporte aos servidores, entre outras. Para tentar minimizar essas falhas, é necessário planejar para evitar os tipos de falhas que forem possíveis.

Neste projeto, os tipos de falhas que serão minimizados serão as falhas de serviços de conexão de dados contratados (Internet ou VPN) e falhas de infraestrutura de execução dos servidores.

3.7.1. Minimizando falhas de conexão de dados

Neste caso, a premissa básica diz que é necessário utilizar duas conexões de dados: uma principal, e outra substituta. Ainda é possível usar as duas conexões sob um regime de balanceamento de carga, ou de agregação de conexões, ambos os recursos são disponíveis em equipamentos específicos. Infelizmente, a aquisição de conexões principais e secundárias para cada uma das unidades encarece demasiadamente o preço final de aquisição, e torna o projeto inviável para a instituição financeiramente. Dado que os sistemas já possuem acesso disponibilizado para a zona da Internet, optou-se por usar esse modelo como conexão secundária, e contratar um serviço de VPN empresarial, com apenas uma conexão para cada unidade.

Neste cenário, temos que, à discricção da direção de TI do Instituto, todas as unidades podem ter duas rotas de roteamento para alcançar os sistemas hospedados no datacenter. Assim, considerando que a rota que passa por dentro da rede de interligação dos campi tem prioridade mais alta, todo o tráfego no sentido campus-datacenter será direcionado por dentro dessa rede de interligação. Caso a conexão do serviço de VPN falhe, a rota que direciona para a Internet passaria a vigorar, mantendo o serviço disponível apesar da falha de conexão da VPN.

3.7.2. Minimizando falhas de infraestrutura

Falhas de infraestrutura podem partir de falhas no hardware ou no software que sustenta os servidores, de acordo com a arquitetura. Considerando uma arquitetura com virtualização, as falhas de software podem envolver problemas com o hipervisor e todos os sistemas que apoiam o seu funcionamento (sistemas de gerenciamento, SAN, entre outros).

Para minimizar isso, a técnica mais comum é a que prevê o uso de redundâncias. Redundâncias podem ser de hardware, de software, de rede, de armazenamento em disco, de gerência, para citar as mais comuns.

Neste projeto, a intenção é utilizar tantas redundâncias quanto forem possíveis, a fim de reduzir ao máximo os riscos de falhas na infraestrutura.

4. SOLUÇÃO DE DATACENTER BASEADO EM VIRTUALIZAÇÃO

A virtualização de servidores é uma técnica que permite a execução de um servidor (ou mainframe) dentro de um ambiente simulado, que provê ao servidor virtualizado todas as características necessárias à sua execução, da mesma forma que aconteceria caso o mesmo fosse implementado em uma máquina física. O uso dessa técnica permite que um mesmo equipamento execute diversos servidores e ambientes diferentes, otimizando o uso de suas características físicas, provendo economia de investimento em recursos computacionais, e fornecendo possibilidade de isolamento de execução.

Serão consideradas apenas três das principais ferramentas de virtualização mais comuns no mercado, segundo a revista eletrônica ServerWatch: VMware vSphere, Citrix XenServer, e Microsoft Hyper-V.

4.1. Virtualização

A virtualização é uma técnica concebida na década de 1960, e teve a IBM como uma de suas principais pesquisadoras, fornecendo esse tipo de solução para seus mainframes sob a vantagem de poder executar ambientes de produção separados, e assim isolar possíveis problemas, sem comprometer a execução do restante dos ambientes de produção. [GRAZIANO, 2011]

Existem diversos tipos de virtualização, dos quais alguns são:

- De hardware;
- De estação de trabalho;
- De rede;
- De armazenamento de dados;
- De memória.

Neste projeto, o tipo de virtualização desejado é de hardware, com a função específica de virtualizar as máquinas responsáveis por servir os sistemas do Instituto para os usuários finais.

Neste tipo de virtualização, alguns subtipos existem:

- Virtualização completa (todo, ou quase todo, o hardware é simulado)
- Virtualização parcial (apenas parte do hardware é simulado)
- Paravirtualização (o hardware não é simulado, mas cada programa hospedado executa separadamente dos outros)

A paravirtualização tem a execução mais rápida de todas, já que o sistema hospedado tem interação direta com o hardware. A virtualização completa é a mais lenta, já que todos os acessos ao hardware devem ser intermediados pelo hipervisor. A virtualização parcial permite que características de ambas as técnicas sejam aplicadas ao mesmo tempo.

4.2. Soluções para alta disponibilidade

Como alta disponibilidade, entende-se um serviço que possui garantia de funcionamento em um determinado nível pré-acordado. No caso específico do IFRJ, não é um nível de serviço definido previamente em documentos ou políticas internas. Apesar disso, busca-se o cumprimento do conceito de alta disponibilidade dentro de uma estratégia *best effort*, de modo a suprir minimamente as necessidades de TI de um instituto em movimento socioeducativo constante.

Não há a absoluta necessidade de se definir porcentagens altas de disponibilidade para os sistemas, visto que os serviços, embora críticos ao longo do dia, não são absolutamente indispensáveis fora do horário de trabalho, e portanto janelas de manutenção para noites, madrugadas e fins de semana são bastante aceitáveis.

Em termos simples, alta disponibilidade pode ser conseguida através de redundâncias: redundância de acesso à rede, redundância de armazenamento, redundância de hospedeiros para virtualização, redundância de energia elétrica, etc.

4.2.1. Tolerância a falhas

Incluso no conceito de alta disponibilidade está o de tolerância a falhas. Embora aquela seja um conceito bastante importante para o datacenter como um todo, este representa a técnica que vai tornar possível alta disponibilidade a nível de software.

O Hyper-V ainda não possui uma arquitetura de tolerância a falhas robusta o suficiente. A mera capacidade de migração sem reinício já é sofrida, conforme será

discutido na seção 4.4. A solução de alta disponibilidade da VMware é a mais adequada ao trabalho, por apresentar desempenho e funcionamento confiáveis e implementação adequada. Nenhum sistema concorrente tem uma implementação adequada desta funcionalidade.

4.3. Balanceamento de carga

Até o momento, o único hipervisor a apresentar um balanceamento de carga consistente e completo é o da VMware, capaz de balancear a carga de processamento com diversos tipos de orientação, inclusive para economia de energia. Há opções, inclusive, para desligar e religar hospedeiros conforme a demanda de recursos.

4.4. Migração de VMs sem reinício

Esta funcionalidade é básica e está presente em praticamente todas as soluções de virtualização presentes no mercado, isto é, as que usam clusterização para servir virtualização. [SHIRINBAB, LUNDBERG, ILIE, 2014]

Há um relatório emitido pela Principled Technologies² sobre testes comparativos entre Hyper-V e VMware, sobre migração ao vivo de máquinas virtuais. De acordo com esse relatório, o Hyper-V teve um desempenho até 5,4 vezes pior em tempo de migração do que a VMware, e causou falhas nos sistemas operacionais das máquinas virtuais em sistematicamente todas as iterações do teste, embora nem sempre na mesma máquina. Já o produto da VMware não resultou nenhum erro.

4.5. Outras opções

De acordo com tabela personalizada emitida pelo site Virtualization Matrix³, contendo dados comparativos sobre cada sistema de virtualização, pode-se observar a cobertura muito mais ampla do VMware em relação a qualquer outro concorrente. As diferenças existem, principalmente, no tangente a tolerância a falhas, caracterizando a

² Fonte: <http://www.vmware.com/files/pdf/vmw-vmotion-verus-live-migration.pdf> (em 20 de outubro de 2014)

³ Fonte: http://www.virtualizationmatrix.com/print_new.php?color=N&prioritize=Y&comment=N&free_based=1&sr_category=General~Management~VM+Mobility+and+HA~Hypervisor~Network+and+Storage&name_company=&name_contact=&ref_project=&date= (em 21 de outubro de 2014)

VMware como a única a oferecer um sistema de tolerância a falhas com possibilidade de *downtime* inexistente em caso de falha de hospedeiro.

4.6. Soluções disponíveis

Existem diversas soluções disponíveis no mercado, com variados graus de funcionalidade e gerenciamento. Há sistemas de virtualização empresarial altamente completos e complexos, como o VMware vSphere, e sistemas de virtualização pessoal simples e triviais como o VMware Player.

Na gama de soluções empresariais, os principais candidatos a solução são o VMware vSphere, o Citrix XenServer, e o Microsoft Hyper-V. Existem outras soluções como a da Oracle VM Server, porém optou-se por verificar as mais expressivas no mercado.

De acordo com as análises anteriores feitas pela equipe de TI do Instituto, e em vista das demandas e necessidades do mesmo por robustez, confiabilidade, flexibilidade de configurações, e estabilidade nas operações, foi escolhida a solução VMware vSphere, por apresentar o melhor suporte ao hardware apresentado [TECHCOMPARISON, 2014], e o melhor equilíbrio de ofertas entre todas as funcionalidades desejadas, isto é, consegue atender bem a todos os requisitos da equipe de TI do IFRJ.

5. ARQUITETURA IMPLEMENTADA NO IFRJ

Após observar o panorama tecnológico do IFRJ, e verificar a viabilidade e a aplicabilidade das soluções disponíveis no mercado, é necessário escolher a melhor solução para implementação, e implementá-la.

5.1. Arquitetura anterior

O Instituto, tendo surgido a partir de uma escola técnica em Nilópolis, e agregando campi já existentes, passou por um período de extensa heterogeneidade de sistemas. Cada campus era responsável pela sua própria ligação à Internet, alguns deles sendo detentores de seus próprios servidores e serviços internos. Não havia uma documentação que demonstrasse o estado corrente do parque de TI dos campi, à época, e foi necessário compreender alguns aspectos das operações dos campi, dentro de suas informalidades, antes de prosseguir com o projeto.

5.1.1. Infraestrutura de rede

Novamente, não havia uma documentação específica que descrevesse e relacionasse todos os sistemas de acesso à Internet utilizados pelos campi. Houve qual fizesse acesso à Internet através de quatro ligações ADSL do tipo doméstica em um sistema de balanceamento de carga. Alguns utilizaram sistemas de ligação principal e ligação reserva, para suprir eventuais quedas da linha principal. Muitos deles tinham problemas constantes com seus acessos à Internet, levando-os a permanecer, às vezes por dias, sem conseguir trabalhar adequadamente por deficiência no acesso aos serviços comuns da Internet.

No momento em que a TI disponibilizou serviços centralizados para todos os campi, a ausência de um sistema de interligação de dados entre eles fez com que todos os serviços e sistemas tivessem que ser disponibilizados diretamente na Internet, via principal de comunicação de dados entre a Reitoria e os campi. Infelizmente, esta via não é confiável, por diversos motivos que englobam segurança, confiabilidade, e estabilidade das ligações de dados. Além disso, as redes internas dos campi, e até mesmo entre os campi, eram bastante heterogêneas, se utilizavam de diversos equipamentos de modelos e marcas diferentes, em tentativas de melhorar o serviço de posse de um orçamento e recursos limitados.

5.1.2. Virtualização

A virtualização era feita usando os sistemas XenServer, hipervisores da Citrix. Funcionavam em máquinas Dell 710R com cerca de 400 GB de HD disponíveis para máquinas virtuais, dois processadores de 6 núcleos cada e 12 GB de memória RAM. Havia um total de quatro servidores Dell com essas configurações, com o mesmo hipervisor instalado em todas, embora as máquinas funcionassem isoladamente. A maioria das máquinas virtuais eram sistemas Linux, e portanto podiam ser restritas a HDs virtuais menores. A máquina virtual onde funcionava o serviço de diretório de usuários, servidor de impressão e sistema de arquivos possuía um sistema operacional Windows, e dada a natureza do sistema, e da função de servidor de arquivos, tinha q ser armazenada em um HD maior. Por esse motivo, esta máquina era a única que executava sozinha em um hospedeiro de virtualização, de modo a tomar todo o HD do hospedeiro.

A gerência da virtualização era feita individualmente por máquina hospedeira, através do software XenCenter. O software permitia um certo grau de liberdade na gerência dos hospedeiros e das máquinas virtuais, e atendia minimamente às necessidades de administração do datacenter, fornecendo histórico de dados limitado de desempenho do hipervisor, tarefas simples de criação, exclusão e modificação de máquinas virtuais. Além dos controles de início, pausa e interrupção de máquina virtual, também fornecia snapshots e um controle simples dos snapshots existentes.

5.1.3. Serviços

Entre os serviços oferecidos à época estavam:

- Servidor Windows com diretório de usuários, servidor de arquivos, servidor de impressão, servidor DHCP, servidor DNS, entre outros serviços de apoio a essas funções;
- Servidor Windows com serviço de terminal remoto;
- Servidor Linux com SIGA-EDU;
- Servidor Linux com SIGA-ADM;
- Servidor Linux hospedando a página do IFRJ na Internet;

- Servidores Linux para desenvolvimento das aplicações acima mencionadas;
- Servidor Linux com o sistema de revista eletrônica, destinado às publicações científicas do Instituto.

Os serviços eram, em parte, originários do início do Instituto. Alguns foram implementados depois. Outros iniciaram seu funcionamento antes do IFRJ surgir.

Dada a quantidade grande de máquinas virtuais em funcionamento, e ao limitado espaço em HD disponível para o armazenamento das máquinas virtuais, seus HDs virtuais foram todos restritos ao mínimo possível para o bom funcionamento de cada máquina, ao mesmo tempo preservando espaço em disco no hospedeiro para a eventual criação de máquinas virtuais adicionais.

5.2. Soluções escolhidas

5.2.1. Virtualização

A plataforma selecionada para este projeto foi o VMware VSphere, capaz de fazer a virtualização de desktops, aplicativos e datacenters.

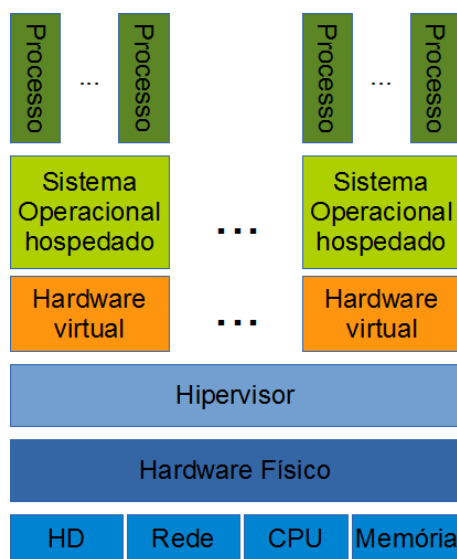


Figura 1 - Hipervisor tipo 1

Os hipervisores são sistemas de gerenciamento de máquinas virtuais, onde são criadas, mantidas e terminadas, e através do qual têm acesso aos dispositivos físicos e

recursos da máquina. O hipervisor não precisa, necessariamente, ser executado isoladamente na máquina; pode também funcionar dentro de outro sistema operacional, de onde tirará os recursos para repassar às máquinas virtuais que gerencia. Dadas suas possíveis formas de execução, são usualmente categorizados em dois tipos: Tipo 1 e Tipo 2.

Os hipervisores do tipo 1, ilustrados na Figura 1, são aqueles que funcionam isoladamente, também conhecidos como "*bare metal*". São executados diretamente após a inicialização da máquina, como se fossem um sistema operacional. A partir dele são executadas todas as máquinas virtuais, e realizadas todas as atividades gerenciais. Exemplos deste tipo são o VMware ESXi, o Citrix XenServer e o Microsoft Hyper-V.

Os hipervisores do tipo 2, ilustrados na Figura 2, são executados de dentro de um sistema operacional previamente existente. A partir dos recursos disponíveis no ambiente onde ele funciona, o hipervisor os repassa para as máquinas virtuais sob ele. Alguns exemplos de hipervisores deste tipo são o Oracle VirtualBox, o QEMU e o VMware Workstation.

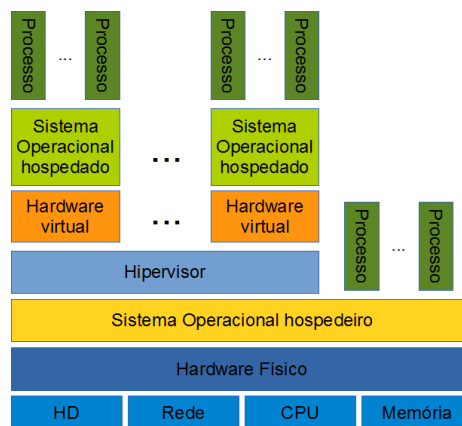


Figura 2 - Hipervisor tipo 2

Um sistema de virtualização pode ser definido como um software utilizado para emular um sistema operacional, ou seja, é um sistema que permite a instalação de sistemas operacionais dentro dele. Desta forma, dois ou mais sistemas operacionais podem ser executados simultaneamente em um mesmo sistema de virtualização. O núcleo da virtualização deste tipo de sistema é o Hipervisor.

Entre as diferentes plataformas de virtualização disponíveis da VMware, uma foi selecionada para a execução deste projeto, a vSphere.

vSphere é uma plataforma de virtualização para a criação de infraestrutura em nuvem. Sua função é tornar recursos de um servidor disponíveis para compartilhamento por diferentes máquinas virtuais permitindo o acesso prioritário com confiabilidade e agilidade. Possui alta disponibilidade, recuperação de falhas para que não haja perda de dados e faz o backup dos dados em disco.

5.2.2. Infraestrutura de Rede

Ao longo dos anos, a fabricante Cisco tem assegurado seu lugar como líder de mercado no segmento dos equipamentos e tecnologias de rede corporativa, tornando-se a mais conhecida, e assumindo papel de referência em redes cabeadas e sem fio. Essa posição tecnológica e de mercado foram decisivas para a escolha quase imediata da Cisco como marca padrão para os equipamentos de rede do Instituto. A resiliência e confiabilidade dos equipamentos, a facilidade de acesso a informações relacionadas ao funcionamento de seus sistemas, e a ampla gama de funcionalidades disponíveis são fatores decisivos para essa escolha.

Nestes termos, optou-se por adquirir e implantar toda a infraestrutura de rede usando switches, roteadores, controladoras de rede sem fio, pontos de acesso e firewalls da Cisco, buscando eliminar todo indício de rede *ad hoc*, facilitando o gerenciamento e rastreabilidade de problemas, e proporcionando um ambiente padronizado e que rivalize com estruturas corporativas de larga escala.

Tabela 2 – Endereçamento utilizado no Instituto, por campus

Grupo	Endereço de rede	Gateway
Equipamentos de rede	10.x.0.0/24	10.x.0.1
Datacenter local	10.x.1.0/24	10.x.1.1
Rede cabeada	10.x.2.0/24	10.x.2.1
Rede VoIP	10.x.3.0/24	10.x.3.1
Rede sem fio interna	10.x.4.0/24	10.x.4.1
Rede sem fio externa	10.x.5.0/24	10.x.5.1
	10.x.6.0/24	10.x.6.1
	10.x.7.0/24	10.x.7.1
Laboratórios (se houver)	10.x.8.0/24	10.x.8.1
	10.x.(...).0/24	10.x.(...).1

Para o endereçamento na rede, desde o núcleo até os computadores, incluindo dispositivos conectados, observou-se a quantidade de equipamentos existentes, de unidades em funcionamento, e a estrutura geral de TI proposta. Com essas características em mãos, e frente à indisponibilidade de endereços IP públicos para atribuição dentro do Instituto, procurou-se, dentro dos endereços existentes na RFC 1918, um que fosse capaz de atender a todas as demandas internas, permitisse espaço para amplo crescimento, e promovesse facilidade de organização, até mesmo para os leigos no sistema de endereçamento IP. Seguindo essas linhas, a melhor escolha foi o espaço de endereços 10.0.0.0/8.

Este espaço de endereçamento deveria ser subdividido em grupos e subgrupos, utilizando o segundo e terceiro octetos para fazer a diferenciação. Sendo assim, o endereçamento ficou:

- Primeiro octeto – prefixo normal da rede 10, inalterado para atender à RFC 1918
- Segundo octeto – indicativo do campus ao qual aquele grupo de endereços pertence, segundo lista pré-estabelecida:
 0. Rede de dados inter-campi (interligação exclusiva);
 1. Campus Maracanã;
 2. Reitoria;
 3. Campus Nilópolis;
 4. Campus Paracambi;
 5. Campus Duque de Caxias;
 6. Campus Volta Redonda;
 7. Campus São Gonçalo;
 8. Campus Realengo;
 9. Campus Agrícola Nilo Peçanha (Pinheiral);
 10. Campus Mesquita;
 11. Campus Engenheiro Paulo de Frontin;
 12. Campus Arraial do Cabo.
- Terceiro octeto – indicativo do tipo de equipamento endereçado, conforme tipos pré-estabelecidos:
 0. Equipamentos de rede;

1. Servidores e dispositivos de acesso geral, localizados no datacenter local;
 2. Computadores e dispositivos cabeados;
 3. Telefones VoIP;
 4. Rede sem fio de uso exclusivo aos equipamentos do Instituto;
 5. Rede sem fio de uso aberto a não funcionários e equipamentos não pertencentes ao Instituto;
 6. Deste número em diante, laboratórios.
- Quarto octeto – dispositivo endereçado;

Este esquema permite identificar rapidamente qualquer endereço IP, principalmente em situações de resolução de problemas, onde um endereçamento críptico pode atrasar, ou até mesmo confundir, a identificação do dispositivo problemático, e conseqüentemente, sua solução também.

Outro benefício deste plano de endereçamento é a capacidade de não depender de tradução de endereços entre unidades. Uma vez que cada dispositivo e equipamento terá um endereço IP único em todo o Instituto, os ativos de rede só terão o trabalho de processar as rotas entre as redes e entre os campi. Comparado à solução anterior, que previa uso de VPNs via software para comunicação intercampi, isso favorece uma redução drástica de latência e tempo de transmissão, pavimentando o caminho para a implantação da telefonia VoIP.

5.3. Ambiente implementado

De posse das soluções escolhidas, as mesmas foram implementadas de acordo com procedimentos específicos de cada tipo de solução. Discute-se aqui o resultado das implementações.

5.3.1. Infraestrutura de Rede

A implementação da nova estrutura de rede foi feita em paralelo: a implementação das redes internas de cada campus seguiu independentemente da implementação da rede MPLS.

Internamente, foram instalados todos os roteadores e switches de acordo com o especificado nas necessidades de cabeamento de cada campus. Os pontos de acesso sem

fio também foram instalados procurando maximizar a área de cobertura de acordo com a geografia e a arquitetura de cada campus. As redes sem fio foram definidas de acordo com o projetado, e configuradas na controladora de APs da Cisco, programada em conjunto com os próprios APs para propagar as configurações de redes sem fio.

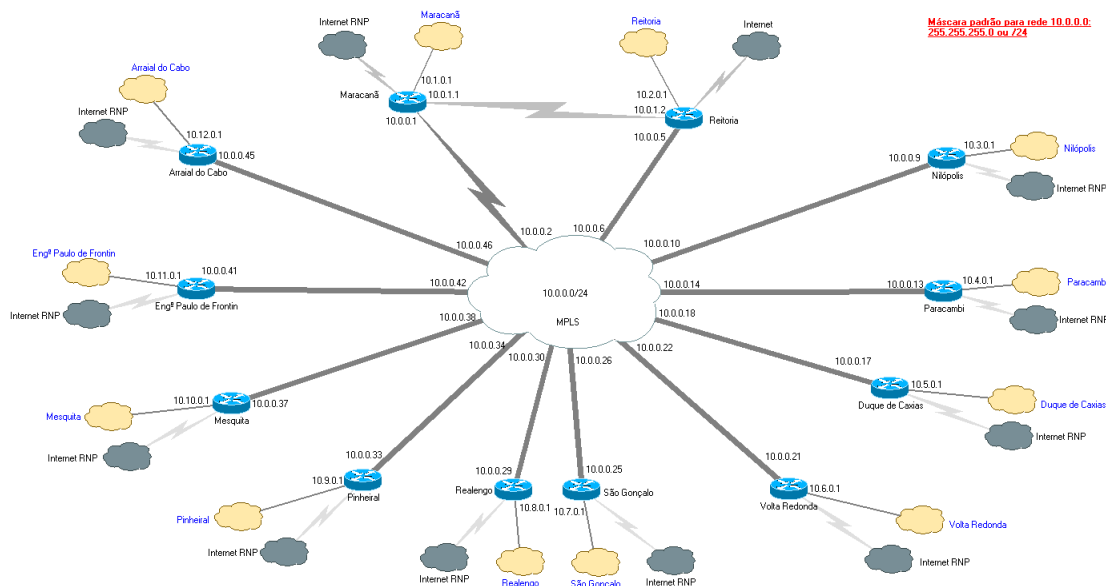


Figura 3 - Topologia de interligação dos campi

A Figura 3 demonstra um esquemático de como a rede ficaria após entrar em operação. Os roteadores desenhados são pertencentes ao IFRJ. Os pertencentes à Oi estão implícitos na nuvem. Seus endereços de rede correspondentes estão denotados nas conexões específicas. Pode-se ver uma prévia da interligação das unidades onde os datacenters estão instalados.

A implementação da rede MPLS seguiu a orientação da Oi para ativações e foi finalizada compreendendo ligações de 2 Mbps para cada campus, e uma de 20 Mbps para o datacenter principal, que também alimenta diretamente o campus Rio de Janeiro. O roteamento por dentro da rede da Oi foi feito utilizando o protocolo BGP para atualização dinâmica das rotas, dentro e fora do Instituto. Não são utilizados firewalls ou outros sistemas de proteção nas ligações MPLS.

As ligações à Internet obedeceram princípios convencionados no IFRJ, que compreendiam a preferência por ligações à internet providas pela RNP, ou entidades

similares/relacionadas. Estas ligações foram implementadas de acordo com o que era negociado, dentro do que era possível à RNP fornecer.

Para provimento de acesso à Internet para os datacenters, foram contratados um link de 4 Mbps *full-duplex* no datacenter secundário, e um link de 8 Mbps, também *full-duplex*, no datacenter primário. Além disso, foi concluída a implantação de uma ligação especial de fibra óptica interligando o IFRJ à Rede Comepi, com a velocidade de acesso de 1 Gbps *full-duplex*. Todos os links possuem grupos próprios de IPs válidos fornecidos pelas suas respectivas empresas.

5.3.2. Sistema de Virtualização

O novo sistema implementado é fornecido pela VMware em conjunto com equipamentos fornecidos pela Dell, em um formato de datacenter de “produção-contingência”, onde um datacenter sustenta as máquinas virtuais operando em caráter de produção, enquanto o outro datacenter permanece sustentando apenas serviços locais, e se mantendo disponível para abarcar os sistemas de produção, caso o datacenter primário venha a falhar por algum motivo.

A solução de virtualização projetada e em funcionamento compreende, em cada datacenter, diversas máquinas físicas em formato de lâminas, operando num mesmo chassis, cada uma possuindo 48 GB de memória RAM, dois processadores de oito núcleos cada um, e dois HDs de 100 GB cada operando em RAID 1 para armazenamento do hipervisor que rodará na lâmina.

Para o armazenamento foram selecionadas, por datacenter, dois módulos de armazenamento de disco, cada um operando com 16 HDs em um formato de RAID 5+0, com variações no tipo de HDs utilizados dependendo do datacenter: no de produção, foram utilizados HDs SAS, de menor espaço, mas maior desempenho; e no de contingência, foram utilizados HDs SATA, com maior espaço e menor desempenho. O sistema de armazenamento ainda previa espelhamento dos conteúdos, de modo que os volumes em operação num datacenter eram espelhados no outro, e vice-versa. Isso garante granularidade na recuperação do ponto de execução das máquinas virtuais.

A Figura 4 demonstra como foram executadas as conexões entre os datacenters. A ligação entre eles foi feita utilizando dois pares de cabos de fibra óptica para interligar exclusivamente os hardwares de virtualização, especificamente os SANs, e mais dois

pares para interligar os equipamentos de rede convencionais (isto é, os equipamentos provedores de rede para usuário final e afins). Nesta figura estão demonstradas apenas as conexões de dados para os servidores virtuais.

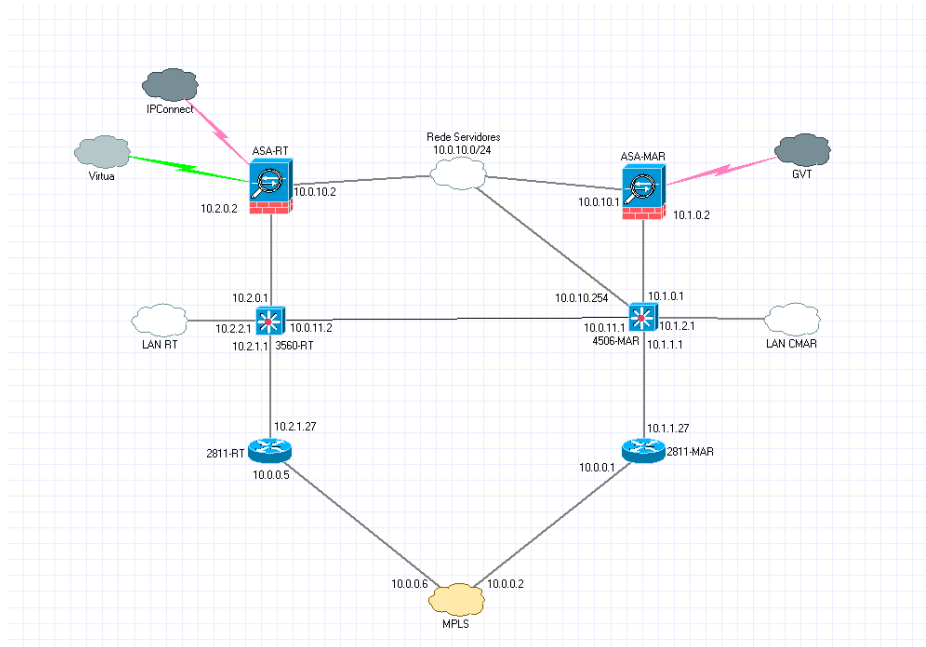


Figura 4 - Topologia de funcionamento da rede do datacenter

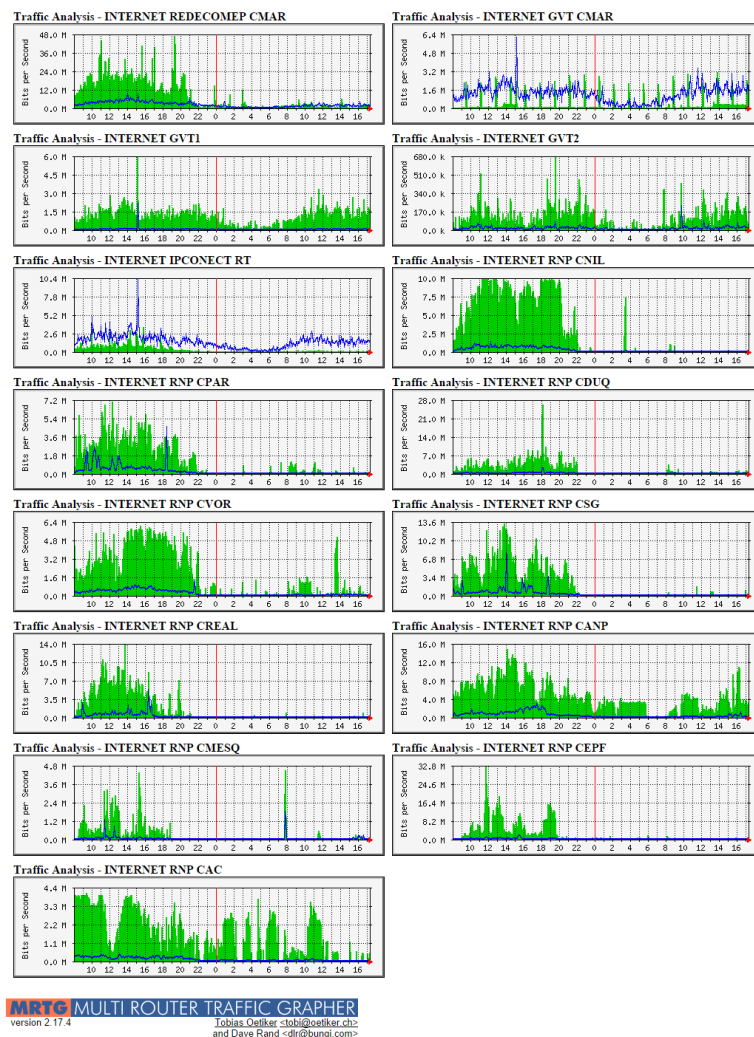
5.3.3. Serviços

Os serviços foram, na verdade, migrados como estavam para o novo sistema de virtualização. Pouca ou nenhuma alteração foi feita em suas configurações originais para que a migração fosse feita. Em última análise, as únicas máquinas virtuais que ofereceram dificuldades para migração foram as que operavam com sistemas operacionais Windows. Dado que não existe migração nativa de máquina virtual do sistema Xen para o sistema VMware, foi necessário utilizar o software Clonezilla para migração das máquinas virtuais com Linux. As máquinas virtuais com Windows, pela expressiva dificuldade em encontrar alternativa viável, tiveram de ser refeitas no sistema de virtualização de destino.

6. FUNCIONAMENTO DA ARQUITETURA IMPLEMENTADA

A implementação da arquitetura proposta, conforme era feita com a paralelização de etapas não dependentes, foi transitando para a fase de produção conforme suas etapas eram encerradas. A Figura 5 traz um exemplo de quinze de outubro de dois mil e catorze, onde pode-se observar as medições dos tráfegos de dados para a Internet através das conexões individuais de cada campus à mesma.

Figura 5 - Exemplo de desempenho das conexões à Internet no Instituto



6.1. Resultado de implementação

Após a implementação, o tráfego de dados entre as unidades e a reitoria teve uma melhora significativa nas questões de segurança e desempenho, garantindo às unidades que todo o tráfego entre os servidores do datacenter principal e as estações de trabalho

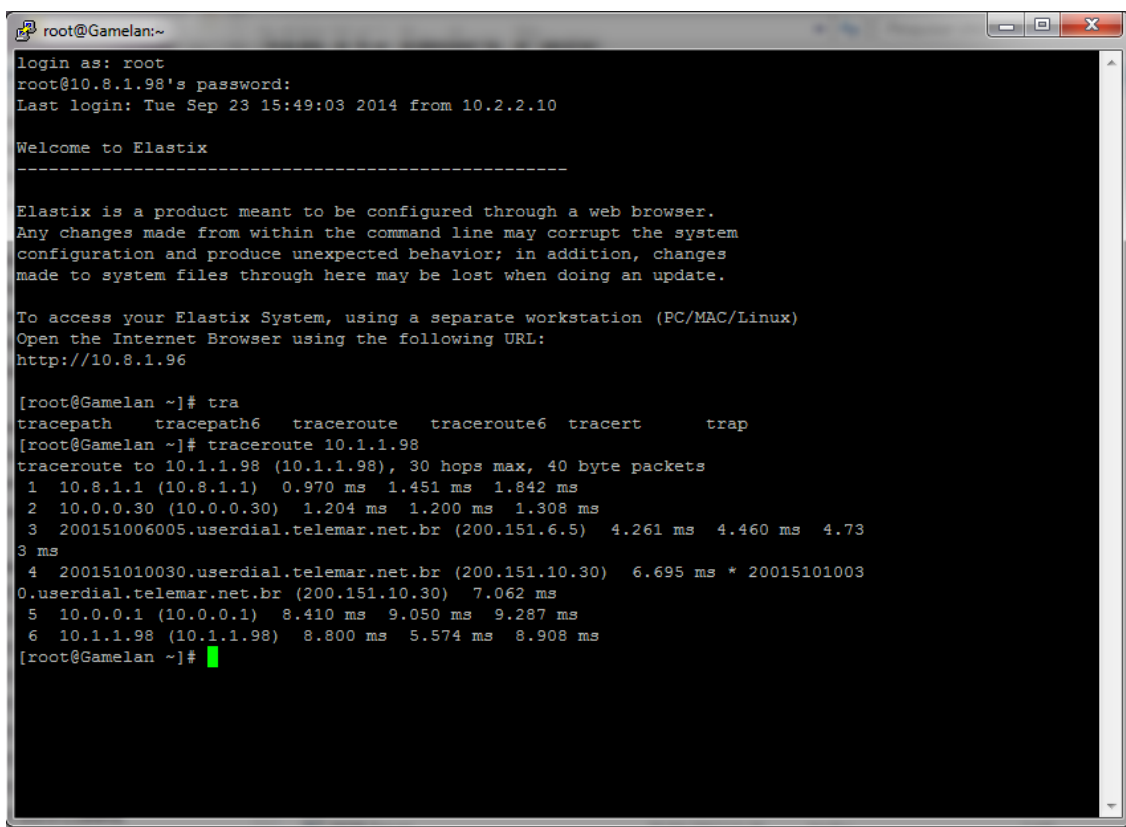
fosse realizado por uma ligação de dados exclusiva e de alta segurança. É possível, também, ter um controle maior quanto à administração do fluxo de dados.

O desempenho no acesso aos serviços disponibilizados pela DGTI no datacenter principal foi melhorado e estabilizado com o uso da rede de interligação. E com a manutenção do acesso aos serviços pela Internet, é possível haver redundância de ligações, reduzindo a quase zero as chances de perda de acesso aos serviços por motivos de falha de ligação com o datacenter.

Esta redundância é possível ao se configurar os roteadores dos campi para direcionar o tráfego com destino aos IPs válidos dos serviços do IFRJ por dentro da rede MPLS. Esse redirecionamento foi feito configurando-se o roteador central, no datacenter principal, para propagar essa rota através de BGP para os outros roteadores. Simultaneamente, cada roteador manteve sua rota padrão para a Internet. Considerando o caminho primário como sendo a MPLS, quando esta sair de operação, a falta de BGP implica na remoção das rotas dinâmicas, deixando a rota padrão do roteador do campus redirecionar todo o tráfego para a Internet.

A Figura 6 é um exemplo de teste de conexão de dados entre dois campi, usando os endereços de dois servidores de telefonia VoIP. O endereço localizado em 10.8.1.98 é do campus Realengo, e o 10.1.1.98 é do campus Rio de Janeiro. Observe que o rastreo passa, na ordem, pelo roteador de núcleo do campus Realengo, pelo roteador de borda da Oi, passa dois pulos sendo roteado por dentro da Oi, emerge no roteador de núcleo do campus Rio de Janeiro, é entregue ao servidor de destino.

Figura 6 - Teste de conexão entre dois campi



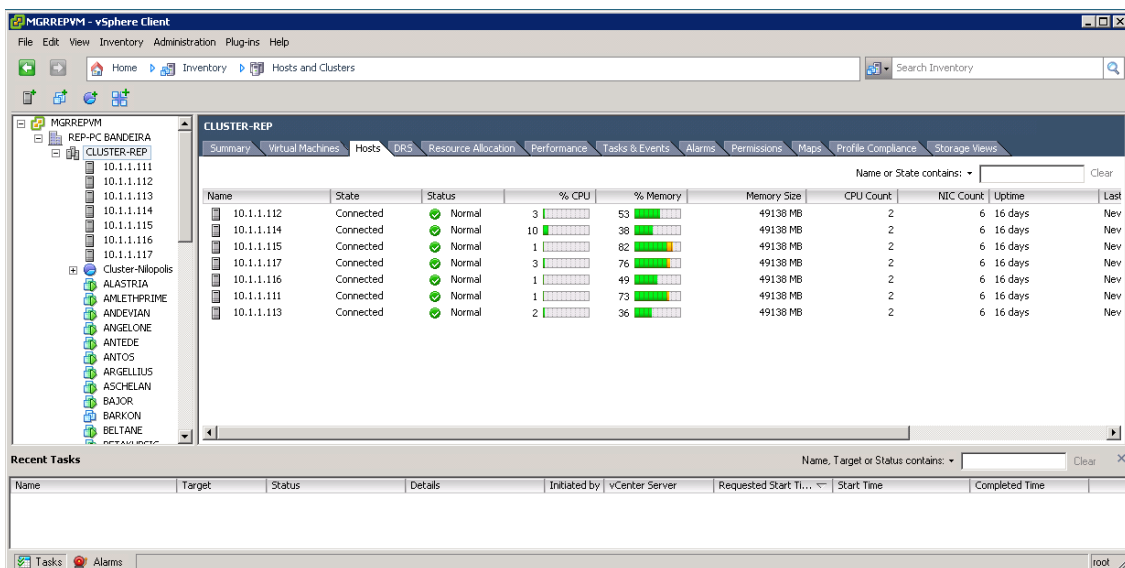
```
root@Gamelan:~  
login as: root  
root@10.8.1.98's password:  
Last login: Tue Sep 23 15:49:03 2014 from 10.2.2.10  
  
Welcome to Elastix  
-----  
  
Elastix is a product meant to be configured through a web browser.  
Any changes made from within the command line may corrupt the system  
configuration and produce unexpected behavior; in addition, changes  
made to system files through here may be lost when doing an update.  
  
To access your Elastix System, using a separate workstation (PC/MAC/Linux)  
Open the Internet Browser using the following URL:  
http://10.8.1.96  
  
[root@Gamelan ~]# tra  
tracepath      tracepath6  traceroute   traceroute6  tracert      trap  
[root@Gamelan ~]# traceroute 10.1.1.98  
traceroute to 10.1.1.98 (10.1.1.98), 30 hops max, 40 byte packets  
 1  10.8.1.1 (10.8.1.1)  0.970 ms  1.451 ms  1.842 ms  
 2  10.0.0.30 (10.0.0.30)  1.204 ms  1.200 ms  1.308 ms  
 3  200151006005.userdial.telemar.net.br (200.151.6.5)  4.261 ms  4.460 ms  4.73  
 3 ms  
 4  200151010030.userdial.telemar.net.br (200.151.10.30)  6.695 ms * 20015101003  
 0.userdial.telemar.net.br (200.151.10.30)  7.062 ms  
 5  10.0.0.1 (10.0.0.1)  8.410 ms  9.050 ms  9.287 ms  
 6  10.1.1.98 (10.1.1.98)  8.800 ms  5.574 ms  8.908 ms  
[root@Gamelan ~]#
```

O advento da ligação de dados entre as unidades permite, também, que se possa redirecionar o acesso à Internet para o datacenter principal, no caso de o link de Internet do campus falhar, e não haver um substituto. À semelhança do método anterior, o roteador pode ter sua configuração alterada, mesmo remotamente a partir de qualquer campus, ou presencialmente, para que sua rota padrão seja modificada para seguir pela MPLS.

6.2. Balanceamento de carga

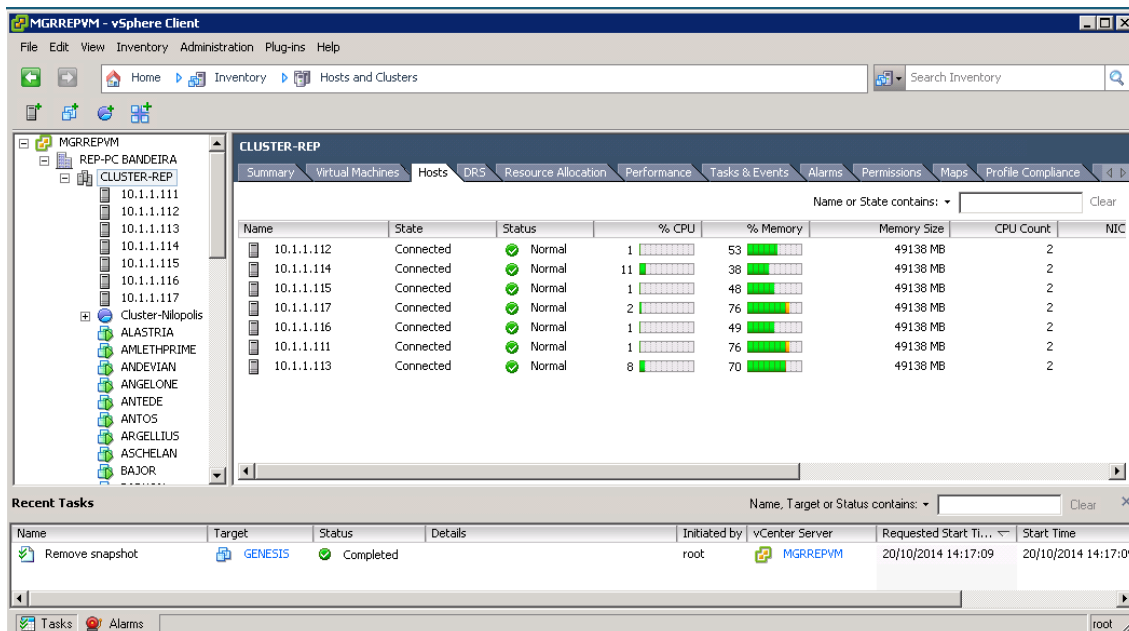
Com um sistema de virtualização com armazenamento unificado por datacenter, e hospedeiros idênticos funcionando sob a gerência de um mesmo servidor de administração, torna-se fácil gerenciar a carga de memória e processamento de cada máquina de virtualização. Caso uma delas apresente sobrecarga de algum recurso, ou se for necessária a criação de uma máquina virtual com requisitos específicos, pode-se aproveitar a possibilidade de migração das máquinas virtuais de um hospedeiro para outro, sem a necessidade de desligar as que estão em funcionamento.

Figura 7 - Hospedeiros antes da migração



Se pode observar na Figura 7 o início de um exemplo de migração. Neste cluster de sete membros, foi migrada uma máquina do hospedeiro 10.1.1.115 para o 10.1.1.113. O resultado da migração pode ser conferido na Figura 8, com as cargas de memória diferentes para os dois hospedeiros.

Figura 8 - Hospedeiros depois da migração



6.3. Usuários

Os usuários, no novo sistema, já não relatam dificuldades em acessar os serviços, principalmente quando há falta de acesso à Internet. Em determinados casos, nem a falha de um link de Internet é capaz de interromper os serviços internos, graças aos métodos de redundância de links por roteamento dinâmico. Isto significa um aumento de resiliência das conexões, o que significa que há a capacidade de oferecer, em um nível institucional, uma garantia de serviço mínima, estipulada com base em métricas e capacidade gerencial.

O serviço de diretório foi expandido. Grupos e usuários tiveram seus espaços de armazenamento expandidos. Alunos e funcionários de entidades externas podem ter suas próprias contas, onde antes apenas estes poderiam ter contas temporárias, e aqueles não podiam de qualquer jeito. Esta oferta foi possível graças à expansão na capacidade de armazenamento do datacenter. Com a nova infraestrutura de virtualização e o novo espaço consolidado de armazenamento no datacenter, é possível oferecer mais espaço de armazenamento, e conceder máquinas virtuais para uso educativo em laboratórios de informática.

Outros serviços de TI obtidos através de parcerias e convênios puderam ser estendidos a todos, tanto técnicos administrativos, como docentes, ou ainda discentes, graças à expansão do diretório dentro da instituição. Um exemplo disso é o serviço Dreamspark, da Microsoft, que distribui licenças gratuitas a funcionários, docentes e alunos de instituições de ensino com propósito educacional. Uma vez que todos podem ter contas, todos podem usufruir deste serviço.

6.4. Limitações de sistema

Quanto à alta disponibilidade, sua única limitação restritiva, atualmente, reside no fato de que, ao ser configurada, ela restringe o número de processadores para apenas um, limitando a possibilidade dos outros sistemas funcionarem com processamento paralelo. Este tipo de habilidade é um diferencial muito importante em algumas aplicações internas. O SIGA-EDU, por exemplo, sendo escrito todo em Java, e necessitando fazer inúmeras consultas a banco de dados, para cada acesso, precisa de processamento paralelo para poder servir as páginas requisitadas com um tempo adequado. Por isso a alta disponibilidade não foi utilizada extensivamente como se imaginava.

Quanto ao funcionamento do próprio sistema de virtualização, existe uma limitação que envolve a dependência de um servidor de gerenciamento para que os hospedeiros possam se manter em sincronia uns com os outros, e manter as configurações corretas, principalmente no tangente ao acesso ao SAN.

6.5. Políticas de segurança

Com o serviço de diretório em funcionamento através do servidor Windows com Active Directory, torna-se possível o estabelecimento de determinadas políticas de segurança para o uso de TI na instituição.

A primeira medida foi esconder determinadas facilidades do Painel de Controle das estações de trabalho, reduzindo o acesso do usuário a um mínimo considerado essencial, como personalizações de área de trabalho e configurações de vídeo e áudio. Foi restrito o acesso a qualquer configuração que fosse diretamente relacionada com o funcionamento do sistema, como configurações de memória virtual, nome de máquina, e acesso à rede. Para se manter um ambiente padronizado e favorecer o foco no trabalho dentro da instituição, optou-se por forçar o uso de um papel de parede específico para todas as estações de trabalho.

Outro benefício gerado pelas políticas de segurança foi a atribuição de impressoras automaticamente para usuários baseado no departamento ao qual pertencem. O departamento, dentro do diretório, aparece como um grupo de usuários, e as impressoras são associadas a esses grupos conforme permissões padrões de uso. Com a política adequadamente configurada, é possível que o sistema identifique a qual grupo pertence o usuário e faça as associações automaticamente dependendo das permissões atribuídas.

O diretório também pode ser utilizado como servidor RADIUS para comunicação com as controladoras de rede sem fio de cada campus, a fim de criar uma SSID particular aos servidores públicos, acessível somente usando informações de usuário e senha para associação do equipamento à rede. Isto trouxe maior segurança à rede, já que os acessos são todos registrados em nome de alguém, e por isso qualquer uso da rede é de responsabilidade da pessoa que possui o usuário em questão.

Uma medida em particular gerou certa polêmica quanto à sua adoção: o bloqueio das portas USB. Uma porta USB disponível para o usuário permitiria a inserção de qualquer dispositivo de armazenamento, e possivelmente um infectado com algum código malicioso. Por outro lado, pendrives e afins são extensivamente utilizados pelas pessoas para fins de trabalho, tendo a própria instituição versões customizadas dos dispositivos.

Os laboratórios de ensino não foram incluídos no domínio inicialmente, já que os esforços de implantação foram direcionados para o ambiente utilizado pelos técnicos administrativos e os professores. Apesar disso, eles estão previstos para serem incluídos futuramente, e poderão ser utilizados pelos alunos, que já têm seus usuários criados no diretório. As políticas relacionadas a eles ainda serão definidas em detalhes, mas poderão ser customizadas de acordo com a aula lecionada.

6.6. Receptividade dos usuários à nova infraestrutura

Antes das mudanças, os usuários tinham plena liberdade com suas máquinas. Os arquivos eram todos armazenados localmente. Qualquer perda de dados deveria ser tratada com a coordenação de suporte local para tentativas de recuperação, dependendo do problema em questão. A rede servia com o único propósito de prover conexão com a Internet e conectar as impressoras que fossem de rede.

As tentativas anteriores de prover um serviço que unificasse o sistema de arquivos em um local compartilhado na rede foram malsucedidas, em parte pela dificuldade de manutenção do sistema, em parte pela pouca evolução desse tipo de sistema à época. Uma das primeiras tentativas nesse sentido foi a implantação de um servidor Nortel, com autenticação e compartilhamento de arquivos. Mas o hardware falhava com frequência, e arquivos eram perdidos com alguma facilidade.

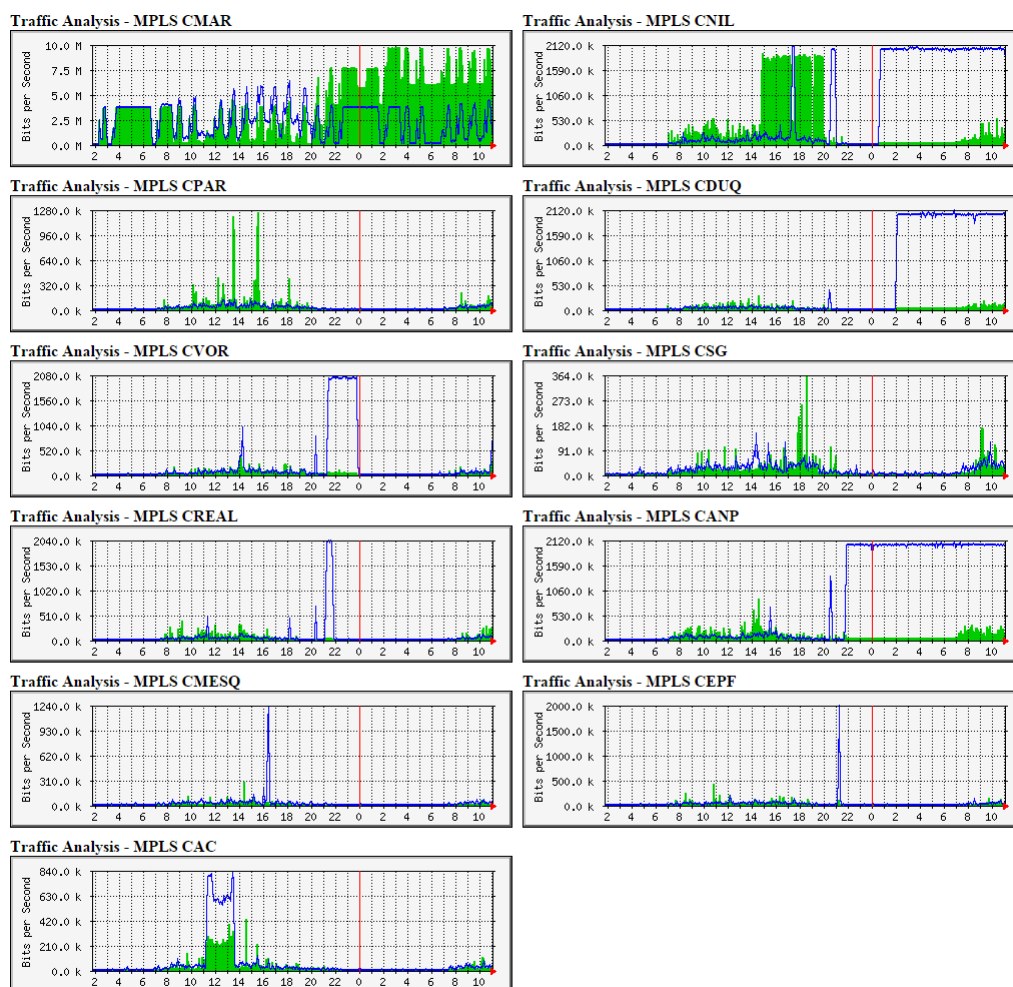
Ao implantar o sistema novo, a comunidade de usuários reagiu, inicialmente, com certa desconfiança. Alguns demonstraram medo de adotar a nova solução pelo histórico de problemas já sofridos anteriormente. À medida que o datacenter entrou em operação, que os serviços começaram a ser oferecidos de forma oficial e estável, e que o sistema se mostrou confiável e resiliente, os usuários foram se acostumando com o novo ambiente, e eventualmente o consideraram uma ferramenta de trabalho útil, passando a usá-lo normalmente, conforme previsto.

6.7. Desempenho geral do sistema

Em termos gerais, o sistema tem apresentado bom desempenho e boa resiliência. O acesso aos discos, que é feito por fibra óptica, apresenta tempos de resposta compatíveis com o uso normal de HDs em máquinas físicas, e não impactam o desempenho das máquinas virtuais.

As redes internas dos campi ficaram bem estruturadas e aptas à expansão, como já tem sido feito nos últimos meses, após o projeto. As redes sem fio têm funcionado de acordo, havendo alguns poucos

Figura 9 - Exemplo de desempenho das interconexões no Instituto



MRTG MULTI ROUTER TRAFFIC GRAPHER
version 2.17.4
Tobias Oetiker <toebi@oetiker.ch>
and Dave Rand <drr@bungie.com>

Como demonstrado na Figura 9, as ligações de dados em funcionamento entre os campi e o datacenter têm sido extensamente utilizadas, indicando que a rede MPLS serve bem aos seus propósitos.

6.8. Futuros objetos de melhoria

Durante e após a implementação do sistema, foram identificados alguns pontos onde é possível investir um trabalho adicional para trazer melhorias ao sistema atual.

Um desses pontos é o serviço de VoIP do Instituto, que hoje ainda usa máquinas próprias para funcionar, mas que já está em pesquisa a possibilidade de mover o sistema de telefonia para uma máquina virtualizada. Atualmente sempre existe, em todos os

campi, uma máquina física dedicada à telefonia IP do IFRJ, por causa dos troncos de E1 que precisam ser conectados no computador através de uma placa PCI específica.

Outro ponto importante é a alta disponibilidade do gerenciador dos hospedeiros. Atualmente ele se encontra numa instalação física de Windows Server em uma das máquinas que seria hospedeira. Isso impossibilita movimentação desse sistema para outras máquinas, e a habilitação de alta disponibilidade para o sistema. Sugere-se a implantação de um sistema único de gerenciamento dos dois datacenters, numa máquina virtual com alta disponibilidade, para maior flexibilização das instalações.

7. CONCLUSÃO

A virtualização é, desde sua criação pela IBM, uma técnica muito importante no desenvolvimento de soluções de TI, principalmente para empresas e instituições de pesquisa. Sua adoção tem trazido benefícios a muitas organizações, nas áreas de gerenciamento de TI, gerenciamento de parque tecnológico, economia de energia, economia de recursos computacionais, monitoramento mais ativo dos sistemas e serviços hospedados, ente outros.

Os benefícios trazidos por esta técnica podem acabar se tornando malefícios, se cuidados básicos não forem tomados. Alguns dos cuidados são: a correta identificação das necessidades de processamento de dados, o dimensionamento das necessidades da instituição, a verificação da aplicabilidade das soluções, a conferência das funcionalidades das ferramentas envolvidas para certificar que elas atendem aos requisitos do datacenter e da instituição, etc.

Após o correto dimensionamento do problema a ser solucionado, pode-se partir para a pesquisa de soluções. É muito importante, durante esta fase, não perder o foco daquilo que a organização deseja em termos de requisitos técnicos, assim como procurar os sistemas de virtualização de melhor qualidade.

Conforme pode ser visto ao longo do trabalho, existem diversas opções de virtualização disponíveis no mercado, e após ter verificado as necessidades dos envolvidos no projeto, pode-se prosseguir com a pesquisa pelo melhor sistema, afim de direcionar a escolha para a solução que melhor satisfará.

Existem soluções de virtualização que variam de simples e pessoais, até complexas e empresariais. É necessário verificar os parâmetros específicos de cada uma, como o tipo de virtualização, sistemas operacionais convidados suportados, funcionalidades de gerenciamento e de alta disponibilidade, entre outros, para conferir a aplicabilidade da solução.

A implementação da solução é de suma importância, já que representa o ápice de todo o trabalho do projeto. Nesta fase tem-se um real vislumbre do alcance da solução e de sua capacidade de atender aos requisitos pré-estabelecidos. Um bom planejamento resulta em uma resposta positiva, o que foi o caso neste projeto. Os requisitos principais foram atendidos, embora ainda haja espaço para aprimoramento das condições. Ao longo

de toda a implantação, procurou-se manter o maior nível possível de comprometimento com uma execução de alta qualidade do projeto.

A cultura de uso das tecnologias de computação é um fator determinante para a aceitação e o sucesso completo do projeto. É preciso dar atenção às demandas dos usuários para se estabelecer a melhor maneira de movê-los para o novo ambiente. Se o histórico de sistemas implementados não apresenta bons resultados, há de se esperar certa resistência dos usuários sobre mudanças. A respeito disto, a melhor maneira de fazer tal mudança é através de um cronograma de mudanças que contemple uma implantação por vez, e períodos de acompanhamento intercalando implantações, de modo que quaisquer problemas sejam resolvidos e a base de usuários seja “estabilizada”, demonstrando a qualidade e a solidez da estrutura nova.

Futuramente, há espaço para desenvolvimento mais profundo da solução de virtualização, incluindo sistemas de backup, e estendendo suas funcionalidades para abarcar também sistemas de telefonia via rede de dados, conhecidos como VoIP. Há também a possibilidade de evolução da suíte de virtualização para um ambiente de nuvem privada.

8. REFERÊNCIAS

ANDRADE, M. T. de. **Um estudo comparativo sobre as principais ferramentas de virtualização**. 2006. 18 f. Dissertação (Graduado em Ciências da Computação) – Centro de Informática, Universidade Federal de Pernambuco, Pernambuco.

TECHCOMPARISON **TechComparison**. Disponível em: <<http://virt.kernelnewbies.org/TechComparison>>. Acesso em: out. 2014.

CREASY, R. J. The Origin of the VM/370 Timesharing System. **IBM J. Res. Develop.**, [S.l.], v.25, n.5, p. 483490, Sept. 1981. Disponível em: <<http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=5390583&queryText%3Dvm%2F370>>. Acesso em: jun. 2014.

FELLER, D. **XenApp on XenServer Round 2 (Ding, Ding)**. Disponível em: <<http://blogs.citrix.com/2008/07/01/xenapp-on-xenserver-round-2-ding-ding/>>. Acesso em: out. 2014.

FREEVPS. **What Are Virtual Private Servers?** Disponível em: <<http://www.freevps.com/overview.html>>. Acesso em: out. 2014.

GRAZIANO, Charles David. **A performance analysis of Xen and KVM hypervisors for hosting the Xen Worlds Project**. (2011) Dissertação e Tese de Graduação. Paper 12215. Disponível em: <<http://lib.dr.iastate.edu/cgi/viewcontent.cgi?article=3243&context=etd>>. Acesso em: out 2014

GONÇALVES, D. B. VAHL JUNIOR, C. **White Paper – Virtualização**. Disponível em: <http://www.digitalassets.com.br/anexos/wp_virtualizacao.pdf>. Acesso em: jul. 2014.

IBM. **O datacenter verde**. Disponível em: <www.ibm.com/br/services/cio/optimize/pdf/White_Paper_Final_Datacenter_verde.pdf>. Acesso em: out. 2014.

KELEM, N.; FEIERTAG, R. A Separation Model for Virtual Machine Monitors. In: IEEE COMPUTER SOCIETY SYMPOSIUM ON RESEARCH IN SECURITY AND PRIVACY, 1991. **Proceedings ...**[S.l.]: IEEE, 1991. p 7886.

LAUREANO, M. **Uma abordagem para a proteção de detectores de intrusão baseada em máquinas virtuais**. 2004. 103 f. Dissertação (Mestrado em Informática Aplicada) Centro de Ciências Exatas e de Tecnologia, Pontifícia Universidade Católica do Paraná, Curitiba.

MICROSOFT. **System Resource Costs of HyperV**. Disponível em: <<http://msdn.microsoft.com/enus/library/cc768536.aspx>>. Acesso em: out. 2014.

PRINCIPLED Technologies. **VMware vSphere vMotion: 5.4 times faster than Hyper-V Live Migration**. Disponível em: <<http://www.vmware.com/files/pdf/vmw-vmotion-verus-live-migration.pdf>>. Acesso em: out. 2014.

STRICKLAND, J. **Como funcionam os servidores virtuais** Disponível em: <<http://tecnologia.hsw.uol.com.br/servidor-virtual.htm> >. Acesso em: out. 2014.

TANAKA, W. **VMware's Future Challenge.** Disponível em:<http://www.forbes.com/2008/04/03/virtualizationsoftwarevmwaretechvirtualization08cx_wt_0403vmware.html>. Acesso em: nov. 2014.

SHIRINBAB, S., LUNDBERG, L., ILIE, D. **Performance Comparison of KVM, VMware and XenServer using a Large Telecommunication Application.** Karlskrona, 2014.