Rodrigo Braga Prado

Estudo de Caso: Implantação de estrutura cliente/servidor na empresa Data Press

Monografia de Pós-Graduação “Lato Sensu” apresentada ao Departamento de Ciência da Computação para a obtenção do título de Especialista em “Administração de Redes Linux”

Orientador
Prof. D.Sc. Joaquim Quinteiro Uchôa

Lavras
Minas Gerais – Brasil
2011

Rodrigo Braga Prado

Estudo de Caso: Implantação de estrutura cliente/servidor na empresa Data Press

Monografia de Pós-Graduação "Lato Sensu" apresentada ao Departamento de Ciência da Computação para a obtenção do título de Especialista em "Administração de Redes Linux"

Aprovada em Abril de 2011

_____
Prof. Eric Fernandes de Mello Araújo

_____
Prof. Sanderson Lincohn Gonzaga de Oliveira

_____
Prof. D.Sc. Joaquim Quinteiro Uchôa
Orientador

Lavras
Minas Gerais – Brasil
2011

Agradeço ao meu mestre Dr. Celso Charuri que me ensinou:
"Quando estiver desanimado, é preciso querer,
Quando estiver cansado, é preciso ousar,
E quando estiver ansioso, é preciso calar."
Sem a sua ajuda mestre, esse trabalho dedicado a construção de um mundo bem melhor, não seria possível e mais um ciclo não seria fechado.

Muito obrigado Mestre!

Agradecimentos Gerais

Agradeço primeiramente ao sr. Diogo Martins Baldani e a toda a equipe da Data Press, sem a ajuda de todos dessa valorosa equipe não seria possível a execução desse trabalho.

Agradeço a toda a equipe de docentes e discentes da UFLA, em especial ao sr. Joaquim Quinteiro Uchôa pelo profissionalismo e grande paciência demonstrada. Mesmo após quatro mudanças de temas e três orientadores diferentes, sempre estava disposto a ajudar.

Meus agradecimentos também a toda a comunidade que acredita, adota e colabora com o crescimento do *software* livre no mundo.

A todos o meu muito obrigado!

Sumário

Lista de Figuras

Lista de Tabelas

Resumo

O presente trabalho tem por objetivo demonstrar como foi realizada a implantação de um sistema cliente/servidor na empresa Data Press, compreendendo um sistema de banco de dados, servidor de arquivos com antivírus integrado, servidor de FTP e um sistema de *proxy* com controle de conteúdo além de um sistema de *backup* dos dados. As redes foram segregadas para uma maior segurança dos funcionários, servidores e dos clientes que acessam um *hotspot*.

O presente trabalho tem por objetivo demonstrar como foi realizada a implantação de um sistema cliente/servidor na empresa Data Press, compreendendo um sistema de banco de dados, servidor de arquivos com antivírus integrado, servidor de FTP e um sistema de *proxy* com controle de conteúdo além de um sistema de *backup* dos dados. As redes foram segregadas para uma maior segurança dos funcionários, servidores e dos clientes que acessam um *hotspot*.

Palavras-chave: Redes, Segurança, Compartilhamento, Virtualização

Capítulo 1: Introdução

Apesar das diversas crises em que o Brasil vem enfrentando ao longo dos anos, várias empresas conseguem crescer. Esse crescimento leva a modernização de processos e dos equipamentos das empresas. Nesse contexto, o autor desse texto foi contratado para realizar o projeto na empresa Data Press para a configuração de um servidor que atendesse a necessidade de crescimento da empresa, com maior segurança, disponibilidade e escalabilidade de seus processos.

A Data Press é uma empresa de impressões gráficas e editora, sediada na cidade de Ourinhos/SP, que realiza diversos tipos de trabalho de impressões como plantas em CAD, *banners*, *folders*, etc. Esses impressos são criados por seus inúmeros clientes que enviam os arquivos finais de seus trabalhos para a impressão em formato digital. A forma de envio mais usual é o *e-mail* ou um formulário no *site* da empresa onde os clientes podem realizar o *upload* do arquivo diretamente para o setor de impressões.

A estrutura de rede inicial dessa empresa consistia em um *link* de Internet ADSL ligado a um roteador *wireless* usando o sistema de criptografia WEP, sendo que apenas uma das estações de atendimento tinha acesso ao *e-mail* da empresa e aos arquivos de impressão dos clientes. Os demais computadores da rede realizavam acesso remotos desses arquivos através de um diretório compartilhado na rede.

O objetivo desse trabalho é demonstrar como foi realizado a implantação de uma nova estrutura de rede nessa empresa, configurado um servidor de baixo custo. Esse servidor efetua o controle de conteúdo de Internet dos terminais de atendimento, e aloca os trabalhos enviados pelos clientes diretamente no diretório compartilhado de rede, sem mais recorrer a retransmissão via e-mail. Fica demonstrado por meio deste que é possível se ter um serviço de qualidade e segurança, normalmente presente apenas em empresas de grande porte.

Para a realização desse trabalho foi realizado uma pesquisa das tecnologias baseadas em *software* livre que atenderiam o projeto, a mesma foi realizada com a leitura de artigos técnicos, manuais dos referidos programas e guias de melhores práticas de cada sistema utilizado.

O presente trabalho segue a estrutura baseado nas normas da UFLA para produção de TCC (PRPG/UFLA, 2007) e está organizado da seguinte forma: no Capítulo 2 são levantados todos os conceitos envolvidos no trabalho. No Capítulo 3 é demonstrado como foram divididos os serviços, os servidores, a segregação das redes. No Capítulo 4 é demonstrada com foram realizadas as configurações dos aplicativos utilizados para a realização desse trabalho. Por fim, no Capítulo 5 são apresentadas as conclusões e análises sobre a implementação realizada.

Capítulo 2: Conceitos Básicos

Serão abordados as teorias que foram utilizadas como base para a elaboração desse trabalho. Posteriormente, será demonstrada como foram implementadas todas as tecnologias na prática.

2.1 CentOS

CentOS[1] é uma distribuição GNU/Linux voltada ao mercado empresarial, baseada no código fonte do sistema Red Hat Enterprise Linux, sendo uma versão livre, que foi disponibilizada e compilada a partir da versão comercial Red Hat Enterprise Linux. As únicas alterações em relação a versão comercial desse sistema são as remoções dos logotipos e marcas registradas da Red Hat Inc.

Um programa compilado para o Red Hat Enterprise funciona no CentOS, sem a necessidade de modificações. As configurações de ambos os sistemas são idênticos, fazendo que toda a documentação do Red Hat Enterprise se aplique ao CentOS.

Por ser um sistema voltado a empresas o CentOS possibilita opções de virtualizações, tendo o Xen[2] já integrado em seu instalador na

1 O CentOS esta disponível em http://www.centos.org
2 Xen - http://www.citrix.com
Xen Source - http://www.xensource.com

versão 5.5. Contando com a opção da instalação posterior de outros virtualizadores como o KVM[3], OpenVZ[4], entre outros.

2.2 Xen

A virtualização permite que em um único servidor físico sejam executados diversos outros ambientes, simulando toda a infraestrutura de um computador, como se fossem computadores completos, como descrito em (LUCAS, 2008). Segundo (MATTOS, 2008), a virtualização não é uma técnica nova, já vem sendo utilizada desde o final de 1960, nessa época apenas nos *mainframes*[5]. Sua utilização visa um melhor aproveitamento do hardware existente reduzindo a sua ociosidade, como descrito em (GOLDEN & SCHEFFY, 2008, p. 3).

Com uso da virtualização, é possível se realizar diversas tarefas com uma menor quantidade de ativos na rede, reduzindo assim o seu custo, tanto de aquisição quanto na manutenção como foi descrito em (SIQUEIRA, 2007, p. 4) e (BIGNES, 2009). A virtualização atualmente, já permite que sejam executados sistemas operacionais diferentes de seu hospedeiro.

A virtualização pode ser realizada de várias formas, as principais são: virtualização total e paravirtualização. No caso da virtualização total,

3 Kvm - http://www.linux-kvm.org
4 OpenVZ – http://www.openvz.org
5 Mainframe é um computador de grande porte, dedicado normalmente ao processamento de um volume grande de informações.

é criada uma camada de abstração do *hardware* que permite a utilização de arquiteturas diferentes de seu hospedeiro em seus clientes. Na paravirtualização o sistema hospedado tem o seu sistema operacional modificado para que possa interagir com o *hardware* do sistema hospedeiro, com isso a sua performance é sensivelmente maior do que em sistemas totalmente virtualizados.

Existem diversas ferramentas de virtualização disponíveis no mercado, algumas são proprietárias e outras são livres. O autor desse texto sempre que possível se utiliza de *software* livre em seus projetos, e entre os virtualizadores[6] disponíveis foi optado pelo sistema hipervisor Xen.

Segundo os próprios desenvolvedores:

> *"O hipervisor Xen é uma camada de software que roda diretamente sobre o hardware do computador e substitui o sistema operacional, permitindo assim que o hardware do computador execute diversos sistemas operacionais convidados simultaneamente.*
>
> *A comunidade Xen.org desenvolve e mantém o hipervisor Xen como uma solução gratuita sob a licença Licença GNU/GPL."*[7]

---

6 Principais virtualizadores do mercado:
VMWare - http://www.vmware.com
Xen - http://www.citrix.com
Xen Source - http://www.xensource.com
Kvm - http://www.linux-kvm.org
OpenVZ – http://www.openvz.org

7 Tradução livre do texto "What is Xen"

O sistema de virtualização Xen possibilita realizar tanto a virtualização completa como a paravirtualização. A opção escolhida pelo autor para a execução desse projeto é a paravirtualização, por permitir uma maior performance em relação a virtualização total, mantendo uma performance muito próxima ao *hardware* do hospedeiro.

2.3 Iptables

O *firewall* é uma combinação de *software* e *hardware* que tem por objetivo proteger as redes e os seus dados de acessos não autorizados previamente (NAKAMURA, 2007). Com isso qualquer pessoa que tente obter dados sigilosos da empresa, até mesmo funcionários não lograrão êxito, mantendo a confidencialidade dos dados e a rede segura de ataques externos e internos (CHESWICK, 2005). Atualmente os ataques internos vem se tornando o maior problema para os administradores de sistemas e redes (FARIAS, 2009).

O Iptables é uma interface para o módulo netfilter do *kernel* do GNU/Linux que provê as funcionalidades de um *firewall* ao GNU/Linux e é executado em um modo não privilegiado, chamado de *userspace*, tornando-o ainda mais seguro. Por ser integrado ao *kernel*, a sua performance é excepcional, além de ser altamente robusto e flexível, servindo perfeitamente aos propósitos desse trabalho.

2.4 Squid

O *proxy* é um servidor que atende a requisições de um cliente, repassando os dados à frente. Hoje na maioria das vezes é utilizado para realizar o trabalho de prover páginas da Internet replicadas dos servidores originais para clientes de outras redes conforme descrito em (MARCELO, 2006). Uma das principais soluções para *proxy* é o *software* livre Squid[8].

O Squid, além de ser um servidor *proxy*, realiza o serviço de *cache*, ou seja armazena as páginas já acessadas em disco para quando um outro cliente realizar a requisição dessa mesma página seja enviada diretamente, aumentando assim a velocidade de navegação. O Squid também é considerado um *firewall* de aplicação. Através dele é possível restringir o acesso a alguns usuários, conteúdos ou pelo tipo de mídia (MORIMOTO, 2008).

2.5 NTP

NTP quer dizer *Network Time Protocol*, e é regido pela RFC 1305[9] É um protocolo sofisticado, como já aponta (BILL FENNER, 2004), e realiza o trabalho de sincronização do relógio do servidor, com precisão de milésimos de segundo. Manter a hora dos servidores correta é fundamental para o seu bom funcionamento, já que existem várias tarefas

8 Squid - http://www.squid-cache.org
9 NTP -RFC 1305 - http://www.faqs.org/rfcs/rfc1305.html

que são realizadas através de agendamentos de horários, além de ser possível um melhor diagnóstico de problemas, invasões, etc., através do sistema de *logs* do sistema.

2.6 FTP

O FTP é um protocolo que permite ao usuário acessar e transferir arquivos para e de outro computador pela Internet ou outras redes, e esse protocolo é definido pela RFC 959[10].

Existem inúmeros programas servidores FTP, o escolhido para esse projeto é o ProFTPD[11] por ser um sistema robusto, seguro. Com o seu uso é possível realizar a integração do *web site* da empresa com o servidor FTP local, recebendo os arquivos dos clientes de forma direta.

2.7 Samba

O Samba é um programa de computador, utilizado em sistemas operacionais do tipo Unix, que provê a interoperabilidade dos compartilhamentos de arquivos e impressoras padrão do Windows para Linux e Unix. O Samba é um *Software* Livre licenciado sob a Licença

10 FTP - RFC 959, disponível em: http://tools.ietf.org/html/rfc959
11 ProFTPD - http://www.proftpd.org/

Pública Geral GNU, o projeto Samba é um membro do *Software Freedom Conservancy.*[12]

Substituto completo de um servidor Microsoft Windows para compartilhamento de arquivos, impressoras compartilhadas e demais recursos compartilhados que são utilizadas em redes proprietárias.

2.8 ClamAV

Antivírus é um programa de computador concebido para prevenir, detectar e eliminar programas maliciosos denominados vírus de computadores.

Atualmente a maioria dos vírus de computador procuram escravizar os computadores infectados, criando uma grande rede de computadores infectados. Depois de escravizados esses computadores realizam de forma descentralizada qualquer tarefa designado por seu criador, como um grande *cluster*[13] de servidores. Isso ocorre sem o consentimento ou a permissão de seus proprietários. Essas redes em maioria são utilizadas para o de envio de *spams*[14].

---

12 http://sfconservancy.org/ O *Software Freedom Conservancy* é uma organização sem fins lucrativos que ajuda a promover, melhorar, desenvolver e defender o *software* livre, oferecendo a infraestrutura para projetos de *software* livre.

13 Cluster é um agrupamento de computadores que realizam juntos uma tarefa específica, multiplicando assim o seu poder de processamento.

14 Spam – Mensagens eletrônicas enviadas em massa sem solicitação.

ClamAV[15] é um programa antivírus multiplataforma, baseado na licença GNU/GPL. O ClamAV é bastante rápido e eficaz na detecção e remoção de vírus, além de possuir atualizações diárias de suas definições de novos vírus. Por ser um *software* livre e cumprir bem a sua função foi o sistema de proteção contra os vírus escolhido pelo autor para a utilização nesse projeto.

2.9 Munin

Monitoramento é o ato de supervisionar a evolução ou o progresso de um processo ou programa, afim de se assegurar que ele permaneça ativo e funcional. Registrando, armazenando e relatado o andamento ou falhas do mesmo.

Com o monitoramento é possível realizar a análise do uso regular dos recursos utilizado na rede, e através das tendências de uso identificar pontos com problema ou possíveis gargalos dos recursos utilizados. De posse dessas informações fica muito mais simples programar futuras atualizações quando os recursos disponíveis estiverem chegando ao fim.

Munin[16] é uma ferramenta de monitoramento gráfico dos recursos da rede com interface *web*. Por ser muito modular e de fácil utilização na instalação padrão já conta com uma grande quantidade de gráficos prontos sem a necessidade de realizar nenhuma configuração adicional.

15 ClamAv - http://www.clamav.net
16 Munin - http://munin-monitoring.org/

Por esse motivo o autor do texto optou pela utilização desse sistema de monitoramento em todos os servidores presentes nesse projeto de modernização da rede.

2.10 RAID/MDADM

RAID é a abreviação de *Redundant Array of Inexpensive Disks* (conjunto redundante de discos baratos) ou *Redundant Array of Independent Disks* (conjunto redundante de discos independentes), que é um meio de se criar um subsistema de armazenamento composto por vários discos individuais, com a finalidade de ganhar segurança e desempenho.

A matriz RAID pode ser gerenciada por um dispositivo específico como uma placa controladora de RAID ou então pelo próprio sistema operacional.

Ao se utilizar uma placa controladora se aumenta significativamente a performance dessa matriz, possibilitando em alguns casos efetuar a "troca a quente" dos discos, chamado de *hot swap*[17]. O uso dessa controladora é sempre o mais indicado, porém o seu custo é bem mais elevado.

17 Hot Swap – Capacidade de se realizar a troca de um componente sem a necessidade de se desligar ou parar o equipamento, mantendo-o em pleno funcionamento.

A utilização desse recurso nos servidores propicia uma maior segurança em caso de falha de um dos discos, mantendo os serviços disponíveis mesmo com algum tipo de problema nos mesmos.

O uso da matriz RAID aumenta a segurança contra a perda de dados, porém não se deve confiar plenamente nesse sistema a ponto de se ignorar o uso das cópias de segurança.

MDADM[18] é um programa do GNU/Linux que gerencia matrizes RAID sem a necessidade de uma placa controladora dedicada, realizando a interação entre o sistema operacional e os discos, sendo transparente ao sistema operacional que o utiliza.

O MDADM é um *software* livre licenciado sob GNU/GPL está presente na maioria das distribuições e apresenta uma boa performance no uso, e a recuperação de sua matriz em caso de falha é simples. Por esse motivo o autor utilizou esse programa para aumentar a confiabilidade e disponibilidade.

18 MDADM - http://neil.brown.name/blog/mdadm

Capítulo 3: Modernização da Rede da Data Press

3.1 Comentários Iniciais

O aumento no número de clientes e de trabalhos executados diariamente na Data Press estava chegando ao seu limite já em outubro de 2010. Esse limite não foi atingindo pelos equipamentos da empresa e tão pouco pela quantidade de funcionários, mas sim pela infraestrutura da empresa, impedindo que um maior número de clientes possam ser atendidos com qualidade nos prazos prometidos.

Na Figura 1, pode ser visto o mapa da rede antiga da Data Press.

Figura 1: Rede antiga da Data Press

O uso de uma estação compartilhada que realizava diversas funções como servidor de arquivos, servidor de banco de dados, além da impressão dos trabalhos de plotagem estava tornado toda a rede inviável.

Ao se realizar uma plotagem de grande formato o ERP[19] e o compartilhamento de arquivos simplesmente deixava de funcionar em toda a rede, parando assim toda as atividades informatizadas da empresa.

Dessa forma, a modernização da rede Data Press teve de ser realizada tanto na sua estrutura física, com novos cabos CAT6[20], novos *switchs*[21] *gigabit,* como a adoção e um servidor. Esse servidor realizará a centralização todas as atividades da empresa, tanto com os dados de seu sistema de gerenciamento ERP, quanto os trabalhos de seus clientes e o compartilhamento de Internet para todos os terminais de atendimento.

Com a mudança para um novo prédio, foi realizado a instalação de uma nova estrutura de rede cabeada utilizando o padrão CAT6, que permite que a velocidade da rede atinja 1000mpbs. O mapa físico da rede pode ser visto no *Anexo A* deste trabalho.

Na Figura 2, pode ser visto o mapa da rede implantada na Data Press.

---

19 ERP (Enterprise Resource Planning) são sistemas de informação que integram todos os dados e processos de uma organização em um único sistema.

20 CAT6 é um cabo padrão Ethernet definidos pela Electronic Industries Association e a Telecommunications Industry Association O cabo CAT6 cabo de dados que contém quatro pares de fios de cobre, que utiliza plenamente todos os quatro pares. Suportando velocidades até 1 gigabit por segundo.

21 Switch é um dispositivo utilizado em redes de computadores para reencaminhar módulos (frames) entre os diversos nós.

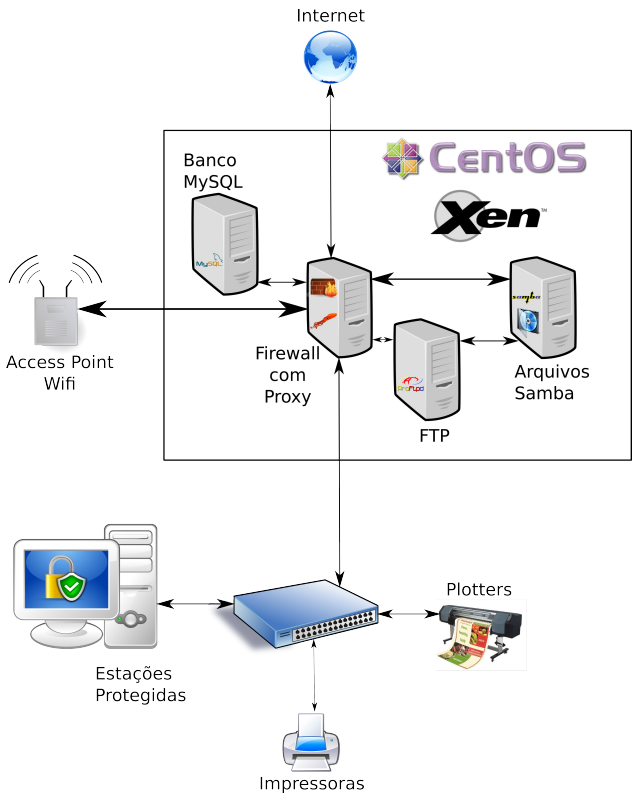

Figura 2: Mapa da Rede Implantada na Data Press

3.2 Servidor Utilizado

Para a implementação da nova estrutura foi adquirido um servidor da Super Micro LT100, com uma placa de rede extra para a segregação da conexão com a Internet. Isso foi necessário porque esse servidor contava com apenas duas placas de rede *gigabit*, e no projeto de migração da rede existem 4 redes distintas, sendo três redes físicas segregadas e uma rede virtual.

O sistema operacional escolhido para a instalação foi o CentOS de 64 bits em sua versão estável que na data de implantação desse projeto se encontra na versão 5.5. Essa distribuição foi escolhida em detrimento da distribuição Debian[22] por não ser 100% suportada pelo fabricante do *hardware* e possuir suporte do distribuidor autorizado no Brasil em casos de eventuais problemas.

O servidor conta com um sistema em sistema RAID 1[23] com dois discos idênticos de 500GB, sendo que o sistema de RAID é gerenciado pelo programa MDADM. O sistema de virtualização escolhido para a execução desse projeto foi o hipervisor Xen. Foram instalados e configurados quatro servidores virtualizados dentro do servidor físico utilizando o mesmo sistema operacional CentOS 5.5 de 64 *bits* que o servidor físico.

3.3 Servidores Virtuais

Os servidores virtuais instalados, usando Xen, seguem o mesmo sistema operacional do servidor físico, CentOS 5.5 na versão de 64 *bits*, e em todos os servidores foram instalados alguns serviços em comum, inclusive no servidor físico, são eles:

22 Debian – http://www.debian.org

23 RAID 1 – Sistema de RAID onde a mesma informação é gravada em dois ou mais discos distintos, mantendo assim a informação em duplicidade para em caso de falha de um dos discos a informação armazenada permaneça acessível pelos outros discos restantes em funcionamento.

- Munin;
- NTP[24];
- Postfix[25];
- Syslog-ng;[26]
- OpenSSH; [27]

Na tabela 1 são listados os servidores e seus respectivos serviços que foram instalados e configurados.

24 NTP – É um protocolo para sincronização dos relógios dos computadores
25 Postfix é um *software* livre para envio e entrega de *e-mails*.
26 Syslog-ng é um *software* livre para registro dos *logs* em sistemas Unix ou GNU/Linux
27 OpenSSH são programas livres que provem acesso a um terminal remoto, transferência de arquivos em uma sessão criptografada utilizando o protocolo SSH.

Tabela 1: Síntese dos Serviços e Servidores

Servidores	IP	Máscara	Gateway	Serviços	
Xen	192.168.10.2	255.255.255.0	192.168.10.1	Xen Munin NTP	SSH Postfix Syslog-ng
Proxy	189.111.123.35 192.168.1.1 192.168.10.1 192.168.11.1	255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0	189.111.123.1	Squid Firewall Munin NTP	SSH Postfix Syslog-ng
FTP	192.168.1.2	255.255.255.0	192.168.1.1	ProFTPd Munin NTP	SSH Postfix Syslog-ng
Samba	192.168.1.3	255.255.255.0	192.168.1.1	Samba Clam AV Munin NTP	SSH Postfix Syslog-ng
MySQL	192.168.1.4	255.255.255.0	192.168.1.1	MySQL Munin NTP	SSH Postfix Syslog-ng

3.4 Firewall de proteção da rede e Proxy

O servidor virtual *Firewall* realiza diversas funções nesse projeto, como a segregação e controle das redes, compartilhamento e controle de conteúdo da Internet da empresa, além de prover a segurança dos dados. Esse servidor conta com um *firewall* personalizado utilizando o programa Iptables, sistema de detecção de intrusão utilizando o programa Snort[28], sistema de *proxy cache* com controle de conteúdo utilizando o Squid e

28 Snort - http://www.snort.org/

sistema de *DNS Cache* utilizando o Bind 9[29]. Além disso, foi instalado um gerador de relatórios de acesso com o programa SARG[30].

3.5 Servidor de Arquivos com sistema de Antivírus integrado

Um dos principais serviços utilizados nesse projeto é o compartilhamento de arquivos. Inicialmente era provido por uma estação de trabalho utilizando Microsoft Windows com um diretório compartilhado e agora é realizado pelo servidor de arquivos. Esse servidor conta com o programa Samba[31] para o compartilhamento de arquivos na rede com o sistema de antivírus ClamAV ativo trabalhando em conjunto, provendo uma maior segurança dos dados nele armazenados.

As definições do antivírus são atualizados de hora em hora através do agendador de tarefas do servidor e todos os dias de madrugada é executada a verificação dos arquivos a procura de vírus nos arquivos compartilhados.

29 Bind 9 - http://www.bind9.net/
30 Sarg - http://sarg.sourceforge.net/
31 Samba – http://www.samba.org/

3.6 Servidor de FTP

O servidor de FTP[32] utiliza o programa ProFTPD para realizar o recebimento de arquivos dos clientes, que são transmitidos através do *site* da empresa. O sistema FTP configurado conta com controle de acessos ao usuários e todos os arquivos são armazenados no servidor de arquivos através de um diretório compartilhado utilizando o sistema NFS[33].

3.7 Sistema de Backup

Foi desenvolvido um *script* para implementação de um sistema de backup personalizado, que realiza a cópia de segurança dos dados de todos os servidores. Esses dados são armazenados em um disco externo ligado a porta *USB*, e todas as vezes que o mesmo é realizado é gerado um relatório que é encaminhado por *e-mail*.

32 File Transfer Protocol, protocolo de transferência de arquivos em rede ou Internet regido pela RFC 959 - http://tools.ietf.org/html/rfc959

33 NFS – Network File System, Sistema de compartilhamento de arquivos em rede que permite o uso de arquivos e diretórios remotos como se fosse arquivos locais, regidos pelas RFCs 1094, 1813, 3530:
http://tools.ietf.org/html/rfc1094
http://tools.ietf.org/html/rfc1813
http://tools.ietf.org/html/rfc3530

3.8 Servidor de Banco de dados MySQL

O servidor de banco de dados utiliza a base de dados MySQL, que é utilizada no sistema de gerenciamento ERP existente na empresa. A adoção de um servidor de banco de dados dedicado trouxe maior agilidade ao sistema ERP implantando, que passa a contar com um servidor dedicado e não mais uma estação de trabalho compartilhada que ao realizar a plotagem de um trabalho parava o sistema de ERP.

Capítulo 4: Configuração dos Serviços e dos Servidores

Nesse capítulo serão abordadas as configurações de cada servidor individualmente e a configuração de cada programa utilizado para a realização desse projeto. O capítulo está dividido em duas partes, a primeira parte a configuração dos servidores de uma forma geral e logo após a configuração de cada serviço presente em cada servidor.

4.1 Configuração dos Servidores

4.1.1 Servidor Físico - Xen

O sistema de virtualização Xen possui seus arquivos de configurações que estão localizadas em /etc/xen. O arquivo de configuração de rede virtual foi personalizado, para que fossem segregadas as redes utilizadas. O arquivo de configuração das redes utilizadas pelo virtualizador Xen se encontra em /etc/xen/scripts/network-bridge-custom.que foi configurado com o conteúdo apresentado na Figura 2.

```
#!/bin/sh
XENDIR='/etc/xen/scripts'

# UP Rede
/sbin/ifconfig eth0 up
/sbin/ifconfig eth1 up
```

```
/sbin/ifconfig eth2 up

# UP VLans - DMZ
/sbin/vconfig add eth0 13

$XENDIR/network-bridge "$@" vifnum=0 netdev=eth0 bridge=xenbr0
$XENDIR/network-bridge "$@" vifnum=1 netdev=eth1 bridge=xenbr1
$XENDIR/network-bridge "$@" vifnum=2 netdev=eth2 bridge=xenbr2
$XENDIR/network-bridge "$@" vifnum=3 netdev=eth0.13 bridge=xenbr3
```

Figura 2: Configuração da rede virtual no Xen

Como pode ser observado no comando *vconfig* foram criadas 4 redes distintas, sendo que uma delas, a rede xenbr3, é uma VLAN[34] da interface de rede ligada a Internet.

Toda a configuração das máquinas virtuais ficam gravadas em /etc/xen/auto, e dentro desse diretório se encontram os seguintes arquivos de configuração:

- aProxy.conf;
- bSamba.conf;
- cMySQL.conf;
- dFTP.conf.

Foi adicionado uma letra antes dos nomes dos arquivos para que seja realizada a inicialização das máquinas virtuais na ordem esperada. Com isso, evitou-se que a montagem do compartilhamento NFS não seja realizado por um dos servidores não estar disponível no momento da montagem do sistema de arquivos do servidor cliente.

34 VLAN – Virtual Local Area Network é uma rede virtual segregada logicamente de uma rede física existente.

4.1.2 Servidor *Proxy-Firewall*

O servidor *Proxy-Firewall* possui o arquivo de configuração /etc/xen/auto/aProxy.conf, esse arquivo controla o servidor virtual *Proxy* com configurações apresentadas na Figura 3.

```
name = "Proxy"
uuid = "a754d565-7f28-f084-96f1-f999b685f824"

maxmem = 512
memory = 512

vcpus = 1

bootloader = "/usr/bin/pygrub"

on_poweroff = "destroy"
on_reboot = "restart"
on_crash = "restart"

disk = [ "phy:/dev/mapper/vms-proxy,xvda,w",
         "phy:/dev/mapper/vms-proxy--cache0,xvdb,w",
         "phy:/dev/mapper/vms-proxy--cache1,xvdc,w",
         "phy:/dev/mapper/vms-proxy--cache2,xvdd,w" ]

vif = [ "mac=00:16:36:00:d6:9c,bridge=xenbr0,script=vif-bridge",
        "mac=00:16:36:00:d7:9c,bridge=xenbr1,script=vif-bridge",
        "mac=00:16:36:00:d8:9c,bridge=xenbr2,script=vif-bridge",
        "mac=00:16:36:00:d9:9c,bridge=xenbr3,script=vif-bridge" ]
```

Figura 3: Arquivo de configuração da máquina virtual *Proxy*

4.1.3 Servidor de Arquivos

O servidor de Aquivos Samba possui o arquivo de configuração /etc/xen/auto/bSamba.conf esse arquivo de configuração do servidor virtual Samba, que conta com dois discos virtuais, um para o sistema e

outro para os dados da rede. As configurações desse servidor virtual são apresentadas na Figura 4.

```
name = "Samba"
uuid = "90a3c054-191e-d391-1575-b4a109ad3e12"

maxmem = 256
memory = 256
vcpus = 1

bootloader = "/usr/bin/pygrub"

on_poweroff = "destroy"
on_reboot = "restart"
on_crash = "restart"

disk = [
        "phy:/dev/mapper/vms-Samba,xvda,w",
        "phy:/dev/mapper/vms-Samba--Dados,xvdb,w"]

vif = [ "mac=00:16:36:5b:77:32,bridge=xenbr3,script=vif-bridge" ]
```

Figura 4: Arquivo de configuração da máquina virtual Samba

4.1.4 Servidor de Banco de Dados MySQL

O servidor de banco de dados MySQL possui dois discos virtuais, um para o sistema operacional e outro apenas para as bases MySQL que serão utilizadas, permitindo assim realizar o aumento ou a troca desse disco virtual por outro de uma forma mais simplificada, sem que seja preciso alterar os arquivos de configuração do banco de dados posteriormente. As configurações desse servidor virtual MySQL estão presentes no arquivo /etc/xen/auto/cMySQL.conf e são apresentadas na Figura 5.

```
name = "MySQL"
uuid = "69fd525b-5e5f-f611-93b3-81155193a7d3"
maxmem = 512
memory = 512
vcpus = 1
bootloader = "/usr/bin/pygrub"
on_poweroff = "destroy"
on_reboot = "restart"
on_crash = "restart"
disk = [
        "phy:/dev/mapper/vms-MySQL,xvda,w" ,
        "phy:/dev/mapper/vms-MySQL--Dados,xvdb,w" ]
vif = [ "mac=00:16:36:42:2c:b7,bridge=xenbr3,script=vif-bridge" ]
```

Figura 5: Arquivo de configuração da máquina virtual MySQL

4.1.5 Servidor FTP

O servidor de FTP possui o usuário datapress com a senha temporária datapress que deverá ser alterado a critério da Data Press com o comando *passwd*. Esse usuário permite o envio de arquivos quando são direcionados ao IP Público 189.111.123.35.

Os arquivos enviados por esse usuário ficam localizados em /files/uploads. O arquivo de configuração do servidor virtual FTP são apresentadas na Figura 6.

```
name = "FTP"

uuid = "0e015543-ae22-b64e-fe21-54c2d5d324c1"

maxmem = 256
memory = 256

vcpus = 1

bootloader = "/usr/bin/pygrub"

on_poweroff = "destroy"
on_reboot = "restart"
on_crash = "restart"

disk = [ "phy:/dev/mapper/vms-FTP,xvda,w" ]

vif = [ "mac=00:16:36:48:c8:df,bridge=xenbr3,script=vif-bridge" ]
```

Figura 6: Arquivo de configuração da máquina virtual *Proxy*

4.2 Configurações dos Serviços

Cada servidor possui os seu serviços e cada serviço possui os seus arquivos de configuração, seguem os serviços de cada servidor bem como os seus arquivos de configuração com o seu conteúdo.

4.2.1 Serviço de Backup

Cada servidor possui um sistema de *backup* idêntico aos demais, o *backup* é realizado em horário agendado no sistema de agendamento do Cron. O script de *backup* esta localizado em /quati/sbin/backup.sh que realiza o *backup* em formato tar.gz e o salva em

/var/www/html/backup/backup-IP_DO_SERVIDOR-dd-mm-aaaa.tar.gz onde dd-mm-aaaa será transformado na data atual como por exemplo: 01-01-2011.

O arquivo de configuração /quati/etc/backup/backup.conf indica o que deve ser salvo no *backup.* Também existe o arquivo de configuração /quati/etc/backups/no_backup.conf que determinar quais as exceções que não deverão ser salvas no servidor. O servidor físico Xen realiza o *backup* de cada arquivo de *backup* de cada servidor e realiza a montagem de um disco externo e transfere os arquivos para o mesmo e mantém durante 7 dias os arquivos no próprio servidor, como medida de segurança.

4.2.2 Serviço de FTP

O servidor de FTP utiliza o *software* ProFTPD para realizar os controle de acessos ao usuários apenas. Todos os arquivos são armazenados no servidor de arquivos e a ligação entre os servidores é realizada através do serviço de NFS. O arquivo de configuração do ProFTPd esta localizado em `/etc/proftpd.conf.`

As restrições de acesso ao diretório compartilhado com o servidor de arquivos são apresentadas nas Figuras 7 e 8.

```
########################
# Usuários de sistema #
######################
DefaultRoot                     /files/uploads/
   <Directory /files/uploads/*>
      AllowOverwrite off
    </Directory>
```

Figura 7: Configuração da restrição de acesso ao diretório dos clientes

```
################################
# Acesso FTP Anônimo com Up Load #
################################
<Anonymous /files/uploads/>
        User                    nobody
        UserAlias               anonymous nobody
        MaxStoreFileSize        200 Mb
        Umask                   000 000
        UserOwner               nobody
        GroupOwner              nobody
        <Limit LOGIN>
                        AllowAll
        </Limit>
        <Directory /files/uploads/*>
                <Limit READ RMD DELE CD>
                        DenyAll
                </Limit>
                <Limit WRITE CWD MKD>
                        AllowAll
                </Limit>
        </Directory>
</Anonymous>
```

Figura 8: Configuração da restrição de acesso a usuários anônimos

4.2.3 Serviço de Compartilhamento de Arquivos

Conforme a solicitação da Data Press, foi criado um compartilhamento sem senha chamado arquivos que aponta para o diretório /files do servidor de arquivos.

O servidor de arquivos utiliza o Samba e o antivírus ClamAV. Os arquivos identificados como infectados são movidos para /files/quarentine.

O arquivo de configuração do Samba esta localizado em: /etc/samba/smb.conf, e a sua configuração básica é apresentada na Figura 9 e o diretório compartilhado é apresentado na Figura 10.

```
[global]
nobody = *
guest account = nobody
workgroup = DataPress
server string = Servidor de Arquivos - %v
netbios name = Arquivos
hosts allow = 127. 192.168.1. 192.168.10.
interfaces = lo eth0 192.168.1.0/24 192.168.10.0/24
log file = /var/log/samba/%m.log
max log size = 50
```

Figura 9: Configurações básicas do Samba para a rede Data Press

```
[arquivos]
comment = Arquivos Compartilhados
path = /files
security = share
public = yes
writable = yes
printable = no
write list = +datapress
read only = no
directory mask = 0750
create mask = 0650
dos filetime resolution = yes
browseable = yes
follow symlinks = true
vfs object = vscan-clamav
vscan-clamav:config-file = /etc/samba/vscan-clamav.conf
```

Figura 10: Configuração do compartilhamento sem senha com o antivírus integrado.

4.2.4 Serviço de *Proxy-Firewall*

Os serviços de *Proxy* e de *Firewall* são realizados pelos programas Squid e Iptables respectivamente, cada qual com seus arquivos de configuração que serão descritos a seguir.

Serviço de Proxy

O servidor *Proxy-Firewall* utiliza o Iptables e o Squid para o sistema de *Proxy* e *Firewall*, além de possuir um sistema de *DNS Cache* utilizando o Bind. O *proxy* Squid possui o arquivo de configuração localizado em /etc/squid/squid.conf. Suas principais configurações serão apresentadas a seguir.

O *cache* de disco é realizado em três discos virtuais e sua configuração é apresentada na Figura 11.

```
cache_dir diskd /cache0 8192 64 64 Q1=64 Q2=72
cache_dir diskd /cache1 8192 64 64 Q1=64 Q2=72
cache_dir diskd /cache2 8192 64 64 Q1=64 Q2=72
```

Figura 11: Configuração do *cache* de Disco, utilizando três discos de *cache*

Para permitir que as atualizações do sistema operacional e das definições do antivírus das estações sejam feitas de forma mais racional, consumindo menos banda de rede, foi criado uma regra de *cache*

especificando o *site* do Windows Update[35]. Dessa forma, as estações foram programadas para realizar as atualizações cerca de 2 horas após a atualização de uma estação específica que foi escolhida arbitrariamente.

Assim os arquivos de atualização já estarão presentes no *cache* de disco e não necessitam efetuar o *download* dos arquivos da Internet novamente. Essa configuração é apresentada na Figura 12.

```
###################
# Cache Microsoft #
###################
refresh_pattern windowsupdate.com/.*\.(cab|exe|dll|msi) 10080 100%
43200 reload-into-ims
refresh_pattern download.microsoft.com/.*\.(cab|exe|dll|msi) 10080
100% 43200 reload-into-ims
refresh_pattern www.download.microsoft.com/.*\.(cab|exe|dll|msi)
10080 100% 43200 reload-into-ims
refresh_pattern www.microsoft.com/.*\.(cab|exe|dll|msi) 10080 100%
43200 reload-into-ims
refresh_pattern au.download.windowsupdate.com/.*\.(cab|exe|dll|msi
) 4320 100% 43200 reload-into-ims
refresh_pattern download.windowsupdate.com/.*\.(cab|exe|dll|msi)
4320 100% 43200 reload-into-ims
refresh_pattern www.download.windowsupdate.com/.*\.(cab|exe|dll|
msi) 4320 100% 43200 reload-into-ims
```

Figura 12: Configuração de *cache* para o Windows Update

35 Windows Update é um serviço de atualização dos sistemas operacionais da Microsoft

A mesma configuração foi realizada para o sistema de atualização de antivírus das estações e é apresentada na Figura 13.

```
################
# AVAST UPDATE #
################
refresh_pattern avast.com/.*\.(vpx|vps) 10080 100% 43200 reload-
into-ims
refresh_pattern -i vpx$ 0 100% 999999 ignore-reload override-
lastmod override-expire reload-into-ims
refresh_pattern -i vps$ 0 100% 999999 ignore-reload override-
lastmod override-expire reload-into-ims
```

Figura 13: Configuração do *cache* para o Antivírus das estações de trabalho.

As páginas de Erros do *Proxy* podem ser customizadas e se encontram em: /quati/etc/squid/Erros_Custom/

Os servidores tem completo acesso à Internet e possuem os IPs cadastrados em um arquivo de controle e o mesmo se encontra em: /quati/etc/squid/acls/servidores_completo.txt.

Os clientes com acesso completo à Internet possuem os IPs cadastrados em um arquivo de controle e o mesmo se encontra em: /quati/etc/squid/acls/lan_completo.txt.

Os *sites* ou termos proibidos de acessarem à Internet possuem um cadastrado em um arquivo de controle e o mesmo se encontra em: /quati/etc/squid/acls/proibidos.txt

Os *sites* ou termos liberados de acessarem à Internet possuem cadastrado em um arquivo de controle e o mesmo se encontra em: /quati/etc/squid/acls/liberados.txt.

Os *sites* ou termos bloqueados de acessarem à Internet possuem um cadastrado em um arquivo de controle e o mesmo se encontra em: /quati/etc/squid/acls/bloqueados.txt.

Os clientes que possuem acesso restrito à Internet possuem um cadastrado em um arquivo de controle e o mesmo se encontra em: /quati/etc/squid/acls/lan_restrito.txt.

Os clientes da rede sem fio tem acesso liberado a maioria dos *sites* para acessarem à Internet possuem um cadastrado em um arquivo de controle e o mesmo se encontra em: /quati/etc/squid/acls/wifi_completo.txt.

Serviço de Firewall

O *Firewall* utiliza o sistema *System V*[36] como padrão e o *software* Iptables para a criação das regras, o arquivo de configuração localizado em /etc/init.d/firewall.

A política padrão adotada nesse firewall é a mais restritiva possível, já que os clientes também terão acesso a Internet mas não devem ter acesso aos dados da rede local da empresa, muito menos ter acesso a rede dos servidores.

Por ser muito extenso serão descritas apenas só trechos mais relevantes do *script* de *firewall* desenvolvido.

Para uma maior agilidade foi adotado uma solução de TOS[37]: para os serviços que causam maior impacto na rede, na Figura 14 estão listadas as opções disponíveis no *script*.

```
MINIMIZE_DELAY="0x10"
MAXIMEZE_THROUGHPUT="0x08"
MAXIMIZE_RELIABITITY="0x04"
MINIMIZE_COST="0x02"
NORMAL_SERVICE="0x00"
```

Figura 14: Configuração das opções do TOS

36 System V – Sistema de inicialização Unix baseada em run levels numéricos e scripts independentes para cada serviço.

37 Type of Services, é um campo no cabeçalho IPv4 utilizado para diferenciar o tipo do pacote a ser transportado, classificando-o para que possa ter prioridade em sua transmissão. É regido pela norma RFC 2474 - http://tools.ietf.org/html/rfc2474

Com as opções configuradas, é possível aplicar as regras como esta apresentado na Figura 15.

```
#######################
# Priorities Protocols #
#######################
$Iptables -t mangle -I PREROUTING -p tcp --dport 21 -j TOS --set-
tos $MINIMIZE_DELAY
$Iptables -t mangle -I PREROUTING -p udp --dport 53 -j TOS --set-
tos $MINIMIZE_DELAY
$Iptables -t mangle -I PREROUTING -p tcp --dport 80 -j TOS --set-
tos $MINIMIZE_DELAY
$Iptables -t mangle -I PREROUTING -p tcp --dport 443 -j TOS --set-
tos $MINIMIZE_DELAY
$Iptables -t mangle -I PREROUTING -p tcp --dport 3306 -j TOS
--set-tos $MINIMIZE_DELAY
$Iptables -t mangle -I POSTROUTING -p tcp --dport 21 -j TOS --set-
tos $MINIMIZE_DELAY
$Iptables -t mangle -I POSTROUTING -p udp --dport 53 -j TOS --set-
tos $MINIMIZE_DELAY
$Iptables -t mangle -I POSTROUTING -p tcp --dport 80 -j TOS --set-
tos $MINIMIZE_DELAY
$Iptables -t mangle -I POSTROUTING -p tcp --dport 443 -j TOS
--set-tos $MINIMIZE_DELAY
$Iptables -t mangle -I POSTROUTING -p tcp --dport 3306 -j TOS
--set-tos $MINIMIZE_DELAY
```

Figura 15: Configuração do TOS para os serviços

O mesmo foi realizado para os serviços de outros servidores, como estão apresentados nas Figura 16 e 17.

```
####################
# Samba Priorities #
####################
# INPUT #
#########
$Iptables -t mangle -I PREROUTING -p tcp --dport 137 -j TOS --set-
tos $MAXIMEZE_THROUGHPUT
$Iptables -t mangle -I PREROUTING -p tcp --dport 138 -j TOS --set-
tos $MAXIMEZE_THROUGHPUT
$Iptables -t mangle -I PREROUTING -p tcp --dport 139 -j TOS --set-
tos $MAXIMEZE_THROUGHPUT
$Iptables -t mangle -I PREROUTING -p tcp --dport 445 -j TOS --set-
tos $MAXIMEZE_THROUGHPUT

$Iptables -t mangle -I PREROUTING -p udp --dport 137 -j TOS --set-
tos $MAXIMEZE_THROUGHPUT
$Iptables -t mangle -I PREROUTING -p udp --dport 138 -j TOS --set-
tos $MAXIMEZE_THROUGHPUT
$Iptables -t mangle -I PREROUTING -p udp --dport 139 -j TOS --set-
tos $MAXIMEZE_THROUGHPUT
$Iptables -t mangle -I PREROUTING -p udp --dport 445 -j TOS –set-
$MAXIMEZE_THROUGHPUT
```

Figura 16: Configuração do TOS para o compartilhamento de arquivos - PREROUTING

```
$Iptables -t mangle -I POSTROUTING -p tcp --dport 137 -j TOS
--set-tos $MAXIMEZE_THROUGHPUT
$Iptables -t mangle -I POSTROUTING -p tcp --dport 138 -j TOS
--set-tos $MAXIMEZE_THROUGHPUT
$Iptables -t mangle -I POSTROUTING -p tcp --dport 139 -j TOS
--set-tos $MAXIMEZE_THROUGHPUT
$Iptables -t mangle -I POSTROUTING -p tcp --dport 445 -j TOS
--set-tos $MAXIMEZE_THROUGHPUT
$Iptables -t mangle -I POSTROUTING -p udp --dport 137 -j TOS
--set-tos $MAXIMEZE_THROUGHPUT
$Iptables -t mangle -I POSTROUTING -p udp --dport 138 -j TOS
--set-tos $MAXIMEZE_THROUGHPUT
$Iptables -t mangle -I POSTROUTING -p udp --dport 139 -j TOS
--set-tos $MAXIMEZE_THROUGHPUT
$Iptables -t mangle -I POSTROUTING -p udp --dport 445 -j TOS
--set-tos $MAXIMEZE_THROUGHPUT
```

Figura 17: Configuração do TOS para o compartilhamento de arquivos – POSTROUTING

Depois dos pacotes serem devidamente marcados com suas respectivas prioridades de processamento, são necessárias as aplicações de regras de restrições ou acessos às redes, na Figura 18 está apresentado o código de acesso a Internet para a rede local.

```
###############
# FORWARD WEB #
###############
$Iptables -A FORWARD -i $LAN_INTERFACE -p tcp -m multiport
--destination-ports 21,25,53,80,110,443,465,995,3128 -o
$WEB_INTERFACE -j ACCEPT
$Iptables -A FORWARD -i $LAN_INTERFACE -p tcp -m multiport
--destination-ports 123,483,563,587,993 -o $WEB_INTERFACE -j
ACCEPT
$Iptables -A FORWARD -i $LAN_INTERFACE -p udp -m multiport
--destination-ports 20,53,443,49152,65534 -o $WEB_INTERFACE -j
ACCEPT
$Iptables -A FORWARD -i $WEB_INTERFACE  -p tcp -m multiport
--destination-ports 21,25,53,80,110,443,483,995,3128 -o
$LAN_INTERFACE -j ACCEPT
$Iptables -A FORWARD -i $WEB_INTERFACE  -p tcp -m multiport
--destination-ports 123,465,563,587,993 -o $LAN_INTERFACE -j
ACCEPT
$Iptables -A FORWARD -i $WEB_INTERFACE  -p udp -m multiport
--destination-ports 20,53,443,49152,65534 -o $LAN_INTERFACE -j
ACCEPT
```

Figura 18: Configuração das regras da Internet

O servidor de arquivos poderá ser acessado somente pela rede interna e não deve ser acessado pela rede sem fio dos clientes, a Figura 19 apresenta o código que garante o acesso apenas à rede local.

```
####################
# FORWARD - SAMBA #
####################
$Iptables -A FORWARD -i $LAN_INTERFACE -p tcp -m multiport
--destination-ports 137,138,139,445 -o $SERVERS_INTERFACE -d
$SERVERS -j ACCEPT
$Iptables -A FORWARD -i $LAN_INTERFACE -p udp -m multiport
--destination-ports 137,138,139,445 -o $SERVERS_INTERFACE -d
$SERVERS -j ACCEPT
$Iptables -A FORWARD -i $SERVERS_INTERFACE -p tcp -m multiport
--destination-ports 137,138,139,445 -o $LAN_INTERFACE -d $LAN -j
ACCEPT
$Iptables -A FORWARD -i $SERVERS_INTERFACE -p udp -m multiport
--destination-ports 137,138,139,445 -o $LAN_INTERFACE -d $LAN -j
ACCEPT
```

Figura 19: Configuração das regras do servidor de arquivos.

O servidor *Proxy-Firewall* possui um sistema de DNS *Cache* utilizando o Bind para que fique independente do DNS da operadora de Internet. O Bind foi instalado em um sistema de chroot[38], isolando assim o DNS do servidor. O Bind utiliza o arquivo de configuração named.conf que está localizado em /var/named/etc/named.conf e possui a opção de DNS-SEC[39] ativada é apresentado na Figura 20.

```
options {
        directory "/var/named/cache";
        auth-nxdomain no;    # conform to RFC1035
        listen-on-v6 { any; };
        dnssec-enable yes;
};
```

Figura 20: Configuração de segurança do DNS-*Cache* com DNS-SEC

38 Chroot é um sistema de jaula em sistemas Unix, não permitindo que o aplicativo acesse outros diretórios que estão fora da jaula, limitando assim o seu acesso ao sistema e melhorando a segurança do mesmo.

39 Domain Name System Security Extensions - Padrão internacional que adiciona ao sistema de resolução de nomes a opção de segurança com criptografia, torando-o assim mais seguro e reduzindo o risco de manipulação de dados e domínios forjados.

O Bind faz referência a outros arquivos de configuração que complementam o mesmo, na Figura 21 é apresentado o arquivo de configuração da Chave do Servidor DNS.

```
rndc.key
key "rndckey" {
        algorithm       hmac-md5;
        secret
"oHaXtZLqhvssNnMhgn5EsPf3LCq7bJrhZxhPM9HApkjUmQibE5UzzgaG70LW";
};
```

Figura 21: Chave do DNS-SEC

Todos os servidores possuem serviços de sincronização de data e hora NTP e o seu arquivo de configuração se encontra em /etc/ntp.conf e é apresentada na Figura 22.

```
restrict default kod nomodify notrap nopeer noquery
restrict -6 default kod nomodify notrap nopeer noquery
restrict 192.168.10.0 mask 255.255.255.0
restrict 192.168.11.0 mask 255.255.255.0
restrict 127.0.0.1
restrict -6 ::1
server a.ntp.br
server b.ntp.br
server c.ntp.br
server 0.centos.pool.ntp.org
server 1.centos.pool.ntp.org
server 2.centos.pool.ntp.org

driftfile /var/lib/ntp/drift
```

Figura 22: Configuração das regras do servidor de arquivos.

4.2.5 Serviço de Banco de Dados MySQL

O servidor de banco de dados MySQL foi configurado com dois discos virtuais, uma apenas para o sistema operacional e outro exclusivo para os bancos de dados. Esse segundo disco fica localizado em /sql.

Para evitar a corrupção dos dados das tabelas também foi adotado a configuração de um arquivo físico para cada tabela, dessa forma se ocorrer algum desligamento abrupto a possibilidade de corrupção da base de dados é menor, essa configuração é realizada com o parâmetro innodb_file_per_table.

O arquivo de configuração do MySQL foi alterado para permitir o uso desse novo disco, o arquivo de configuração se encontra em /etc/my.cnf e o seu conteúdo é apresentado na Figura 23.

```
[mysqld]
datadir =       /sql
socket  =       /sql/mysql.sock
pid-file        = /sql/run/mysqld.pid
log             = /sql/log/mysql.log
log_slow_queries        = /sql/log/mysql-slow.log
skip-bdb
innodb_file_per_table
[mysqld_safe]
socket          = /sql/mysqld.sock
log-error       =       /sql/log/mysqld.log
pid-file        =       /sql/run/mysqld/mysqld.pid

[client]
socket=/sql/mysql.sock
```

Figura 23: Configuração do MySQL utilizando um ponto de montagem diferente do padrão

Capítulo 5: Resultados obtidos

Logo após a implantação do servidor foi constatado um problema de congelamento do servidor quando o tráfego de rede era intenso. Foram realizadas pesquisas que constataram a existência de um *bug*[40] relacionado ao *driver* e1000e.

Foi realizado o *download* do pacote RPM http://elrepo.org/linux/elrepo/el5/x86_64/RPMS/kmod-e1000e-xen-1.2.20_NAPI-1.el5.elrepo.x86_64.rpm e o mesmo foi instalado no servidor, posteriormente foi confirmado se o novo módulo estava ativo nas interfaces.

Antes:

***Driver*:** e1000e

Versão: 1.0.2-k3.1

Depois

***Driver*:** e1000e

Versão: 1.2.20-NAPI

Após a atualização do *driver* o servidor passou a operar normalmente, sem qualquer tipo de anormalidade.

Com a nova estrutura em funcionamento os usuários perceberam de imediato a mudança em todas as tarefas executadas na rede.

A confiabilidade do armazenamento de arquivos aumentou. Anteriormente a estação que armazenava os arquivos era um terminal

40 Bug - http://bugs.centos.org/view.php?id=4371

operacional, sujeito as instabilidades e ataques de vírus do dia a dia. Era muito comum o desaparecimento de arquivos, corrompimento ou a exclusão acidental.

Em comparação ao processo anterior houve aumento de 70% na confiabilidade. Esse aumento só não foi maior por não possuir um operador dedicado a gerenciar este fluxo.

Houve um grande acréscimo no fluxo dos arquivos que transitavam pela rede. Antes a rede ficava lenta com vários acessos agora com o servidor dedicado a queda de desempenho não é notada. Houve um aumento de 200 % no fluxo de informação a adoção do servidor.

Um dos problemas existentes anteriormente é uma limitação das estações com o Microsoft Windows XP, que limita em 8 acessos simultâneos para cada pasta compartilhada, negando assim o acesso após isso. Hoje com a adoção do servidor de arquivos esse limite não exite mais. Anteriormente muitas vezes o usuário ficava aguardando a pasta ser liberada e perdia tempo na produção que teve um aumento de 300%, a rede nesse ponto já estava ficando sobrecarregada.

Não havia regras de compartilhamento e recepção de dados. Após a migração da rede Data Press foram implantadas políticas de acesso, restringindo o acesso não autorizado, como redes sociais, que atrapalhavam o andamento de suas atividades, ficando agora focado em suas atividades principais.

A segurança dos dados eram realizadas sem nenhuma periodicidade. Após a migração os backups são feitos regularmente de

forma automática, além de ser realizado diariamente em um hd externo. Fazendo com que a se ganha-se tempo com a automatização de um processo que antes era feito fora de hora.

Como pode ser visto no relato, houve aumento significativo na velocidade de todos os trabalhos executados na rede, como por exemplo as plotagens. O acesso aos *e-mails* dos clientes ficou facilitado pela descentralização de acesso. O acesso ao ERP melhorou, respondendo prontamente a todas as requisições, não travando mais, mesmo com muitos trabalhos e clientes simultâneos.

As estações de trabalho agora contam com acesso a Internet com controle de conteúdo, e os clientes possuem um *hotspot* para acesso à Internet.

A segurança da rede melhorou, o antivírus no servidor proporciona uma segurança extra aos dados que os clientes enviam.

O antivírus das estações agora são atualizados diariamente, antes a sua atualização era bimensal. O mesmo ocorre com as atualizações do Microsoft Windows que estão agora sempre em dia devido ao uso do *cache* na rede.

O sistema de *backup* agendado em um disco externo se mostrou muito prático, bastando ligá-lo ao servidor na parte da manhã e removê-lo após o recebimento do *e-mail* de sua conclusão com o estado da cópia de segurança em seu relatório.

A Data Press ficou satisfeita com os resultados obtidos com a implantação da nova rede. Existem planos de expansão da empresa a

curto prazo para outra cidade, contando com um servidor semelhante em que serão agregados ainda os serviços de VPN e VoIP para a interligação das unidades.

Capítulo 6: Conclusão

O objetivo desse trabalho foi demonstrar como foi realizada a implantação de uma estrutura centraliza para o controle de uma pequena ou média empresa. Esse mesmo modelo pode ser utilizado em diversas outras empresas de qualquer segmento, já que o sua configuração está muito modular e independente.

A maior necessidade que deveria ser atendida por esse trabalho era propiciar o aumento da velocidade e da disponibilidade dos recursos da rede, permitindo dessa forma o crescimento da empresa.

A adoção da virtualização de servidores permitiu que fosse implementada a infraestrutura com apenas um único equipamento, mantendo baixo os custos de adquisição e posteriores manutenções. Tudo isso sem abrir mão da flexibilidade, segurança e robustez.

Em pouco tempo após a implementação os resultados positivos foram sentidos por todos os usuários da rede, as estações de trabalho estão mais seguras com as constantes atualizações dos seus aplicativos que antes não eram realizados por deixar a rede muito lenta, prejudicando os negócios da empresa.

Esse projeto já prevê em um futuro próximo a adição de novos serviços como VPN e um PABX-IP utilizando a mesma infraestrutura existente, assim que a empresa inaugurar a sua filial.

Referências Bibliográficas

MATTOS, DIOGO MENEZES FERRAZANI. Virtualização: VMWare e Xen, disponível na Internet via http://www.gta.ufrj.br/grad/08_1/virtual/artigo.pdf
Arquivo capturado dia 03 de Abril de 2011.

FLORÃO, LUCAS TIMM, VIRTUALIZAÇÃO COMO ALTERNATIVA PARA AMBIENTE DE SERVIDORES. 2008 - TRABALHO DE CONCLUSÃO DE CURSO FACULDADE DE TECNOLOGIA SENAI DE DESENVOLVIMENTO GERENCIAL – FATESG

GOLDEN, Bernard; SCHEFFY, Clark. Virtualization for Dummies, Sun AMD- Special Edition. Indianapolis: Wiley Publishing INC, 2008.

SIQUEIRA, Luciano; BRENDEL, Jeans-Chistoph. Linux Pocket Pro – Virtualização. São Paulo: Linux New Media, 2007.

BIGNES Eugenio, (2009). Virtualização: um novo conceito de TI, disponível em: http://www.malima.com.br/article_read.asp?id=593, Acesso em 03 de Abril de 2011.

CHESWICK, W. R.; BELLOVIN, S. M.; RUBIN, A. D. Firewalls e Segurança na Internet - Repelindo o Hacker Ardiloso. 2.a edição. ed. Porto Alegre - RS:
Bookman, 2005.

Ranum , Marcus - Thinking about Firewalls. 1994 – Disponível em http://www.cs.ucla.edu/~miodrag/cs259-security/ranum94thinking.pdf

NAKAMURA, E.T., GEUS, P.L. Segurança de redes em Ambientes Cooperativos. Ed. Novatec 2007 (capítulo 7)

Rossoni, Farias
http://tecspace.com.br/paginas/aula/si/aula02.pdf

ANTONIO, MARCELO - SQUID - CONFIGURANDO O PROXY PARA LINUX - Página 3 – 2006 - ISBN 85-7452-269-4

MORIMOTO, C. E. Servidores Linux - Guia Prático. [S.l.]: GDH Press e Sul - Editores, 2008. ISBN 978-85-99593-13-4.

BILL FENNER,W. RICHARD STEVENS,ANDREW RUDOFF - PROGRAMAÇAO DE REDE UNIX, V.1: API PARA SOQUETES DE REDE – 2004 - ISBN 0-13-141155-1

LAUREANO, MARCOS – PROTEÇÃO DE DETECTORES DE INTRUSÃO ATRAVÉS DE MÁQUINAS VIRTUAIS – 2004 – Disponível em http://www.mlaureano.org/projects/vmids/vmids_wseg.pdf

O.K. Takai; I.C.Italiano; J.E. Ferreira.
DCC-IME-USP – Fevereiro – 2005

What is Xen - disponível em : http://www.xen.org/files/Marketing/WhatisXen.pdf

MILLS (1992) MILLS, D. L. Network Time Protocol (Version 3) – Specification, Implementation and Analysis. Internet Engineering Task Force (IETF), Março 1992. (Request for Comments: 1305). Disponível em: <http://www.ietf.org/rfc/rfc1305.txt>. Acesso em: 13 mar. 2011.

Postel, J. - Network Working Group, Outubro de 1985
<http://www.ietf.org/rfc/rfc959.txt>. Acesso em: 13 mar. 2011.

Anexo A

Mapa da Rede Data Press