Solução de Backup em Desktops: Aplicação em Cenário Real

Wanderson Nunes da Rosa[1]

[1]Redes de Computadores
Faculdade de Tecnologia SENAC Pelotas (FATEC)
Rua Gonçalves Chaves 602 – 96015560 – Pelotas – RS – Brazil

wandnrosa@gmail.com

Abstract. *This article aims to present the analysis and restructuring of a backup solution in a large scenario. The selected network environment for the study comprises 25 departments with about of 1300 computers. The hosts are connected between two networks through a variety of communication technologies, but without a proper security handling for file backup solutions and, with it, generating constant complaints from users due to the lack of industry technical administration responsible. The material produced in this article was developed in a real environment, demanding attention in the implementation and serving as a motivational factor for your conclusion.*

Resumo. *Este artigo tem como objetivo apresentar a análise e reestruturação de uma solução de backup em um cenário de grande porte. O ambiente de rede selecionado para o estudo é constituído por 25 secretarias com cerca de 1300 computadores. Os hosts estão interligados entre duas redes por meio de tecnologias variadas de comunicação, porém sem uma tratativa de segurança adequada para com soluções de backup de arquivos e, com isso, gerando reclamações constantes de usuários devido à falta de administração técnica no setor responsável. O material produzido neste artigo foi desenvolvido em um ambiente real, demandando atenção na implementação e servindo como um fator motivacional para sua conclusão.*

1. Introdução

Este estudo baseia-se na análise de implementação de soluções de backup na infraestrutura computacional da Companhia de informática de Pelotas (COINPEL), empresa pública municipal que é responsável pela gerência da rede de computadores da Prefeitura Municipal de Pelotas assim como de todos os seus órgãos públicos.

Tendo em conta que a rede gerenciada pela COINPEL é constituída por 30 subredes interligadas entre si por tecnologias variadas de comunicação, o somatório de hosts destes ambientes atinge, atualmente, 1300 hosts. Visando os constantes avanços tecnológicos aplicáveis, dentre eles a disponibilidade de dados e arquivos de todas as secretarias, incluindo backups pessoais de forma sigilosa, gerando aumento significativo à segurança dos dados, o intuito desse artigo está baseado em uma melhora significativa de toda rede.

Levando em consideração que o cenário atual efetua backups de forma insegura, por vezes não íntegra não automatizada e gerando insatisfações sobre o serviço prestado, a implementação de uma solução de backup se tornou viável para dar otimizar o ambiente e garantir confiabilidade ao usuário.

Ao decorrer do artigo serão apresentadas as definições, visando de forma clara e objetiva atender os requisitos para um entendimento por completo dos testes e do modo que a solução irá beneficiar o ambiente computacional. Tendo em conta que foram realizadas pesquisas bibliográficas e consultas diárias a livros da área de tecnologia da informação para absorção de conhecimentos e técnicas confiáveis para serem aplicadas ao longo do desenvolvimento do relatório.

Entre as importâncias do relatório, estão os esclarecimentos das principais necessidades de correções em medidas preventivas em relação à segurança de dados em empresas e em seus computadores que não podem conter informações cruciais sobre as mesmas, onde essas informações necessitam de um nível adequado de segurança, a fim de evitar futuras situações prejudicais. Dessa forma, o artigo aborda teste de segurança aplicado de forma ética em ambiente empresarial e após o contato com falhas, aborda medidas para sanar as falhas de segurança, onde de forma clara e profissional é executado com êxito.

2. Cenário Atual

Dando início ao projeto foi necessário analisar tecnicamente o cenário da empresa avaliando sua infraestrutura de rede, para que posteriormente fosse gerada a documentação desta tendo em vista que o ambiente é constituído por prédios interligados.

Foram necessários definir alguns ajustes no método de analisar a infraestrutura da rede, sabendo que a rede é dividida entre dois servidores de firewall e DHCP que designam duas faixas de IPs distintas, foram definidos dois ambientes identificados como LADO A e LADO B.

- Total de 650 hosts em cada ambiente (Lado A e Lado B);
- Solicitação de compra de três servidores;
- Mapeamento do cenário de backups.

Os ajustes que vão ser desenvolvidos, conforme citação acima, são somados por anos sem administração correta da rede, com servidores antigos e de pequeno porte, tornando impossível a realização projeto, contudo, foram realizados os levantamentos do que era necessário no primeiro instante, e a solicitação de compra dos mesmos.

Assim como o crescimento do parque computacional a decorrer do tempo, fazendo com que a rede não obtivesse mais endereçamento IP. No diagrama geral da rede, como pode ser visto na Figura 1, é possível observar de qual forma o cenário vai ficar com seus respectivos servidores e a rede ”divida”para melhor administração.

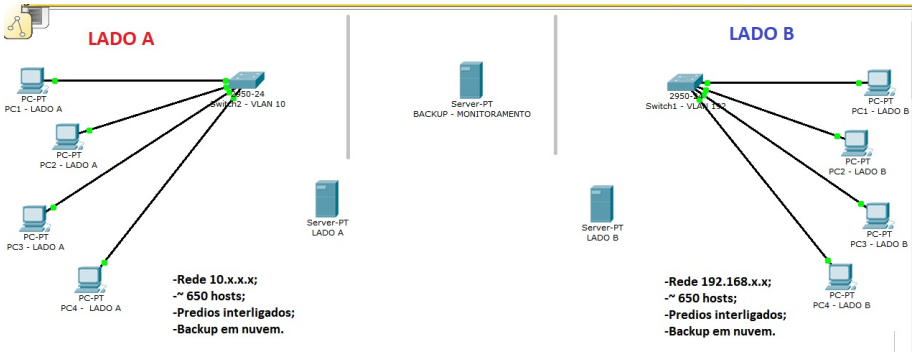

Figura 1. Esboço da Rede

2.1. Análise da Rede

Após o estudo referente a infraestrutura da rede e a organização dos itens citados na seção anterior, foi possível montar a documentação da rede e a estratégia para segmentá-la. Conforme foi analisado o cenário, o mesmo será constituído por dois lados, sendo que em cada lado existem os prédios (secretarias) e seus respectivos computadores.

Sendo que cada lado é dividido por duas faixas de IP para precauções futuras de falta de IP na rede. O grande intuito da solicitação de compra de três servidores baseou-se nos requisitos mínimos de hardware exigidos para armazenamentos de dados de toda a rede computacional.

2.2. Cenário Atual

Como a empresa dispunha no momento de baixo recurso financeiro, a estratégia para implementar a solução de backup com o melhor custo/benefício na rede foi a implementação, com os recursos que eram disponíveis na empresa, uma ferramenta de backup gratuita. Com o levantamento dos dispositivos da rede se adotou como estratégia abranger os backups da rede com uma ferramenta única com o adendo de ferramentas de monitoramento para obter resultados positivos e facilitar a administração da rede.

2.3. Backup

Tendo em vista que no ambiente trafegam dados importantíssimos, atualmente não existe nenhuma solução em backup na empresa, os dados são salvos de forma aleatória, ou por meio de um compartilhamento de total acesso a todos, tendo risco de exclusões acidentais e modificações sem versionamento. No cenário atual, uma vez por semana, um colaborador da empresa realiza o backup do compartilhamento não tendo embasamento referente sobre o que necessário e o que é descartável, e muitas vezes gerando instabilidade para os demais usuários com acesso a rede.

Após uma avaliação e estudo na rede referente à quais formas eram realizados os backups, pode-se observar através da Figura 2 a forma inadequada em que é realizado.

Conforme Figura 2 o cenário está divido em dois lados, no canto inferior esquerdo é apresentado o servidor de origem (fs01-Servidor de Compartilhamento) onde os arquivos serão copiados dele, manualmente, para o servidor de destino (prodbkp02-Servidor de Backup) no canto inferior direito. Onde ambos estão organizados por pastas de seus respectivos setores, porém a forma que estes backups estão sendo realizados está colidindo com os de mais usuários na rede.

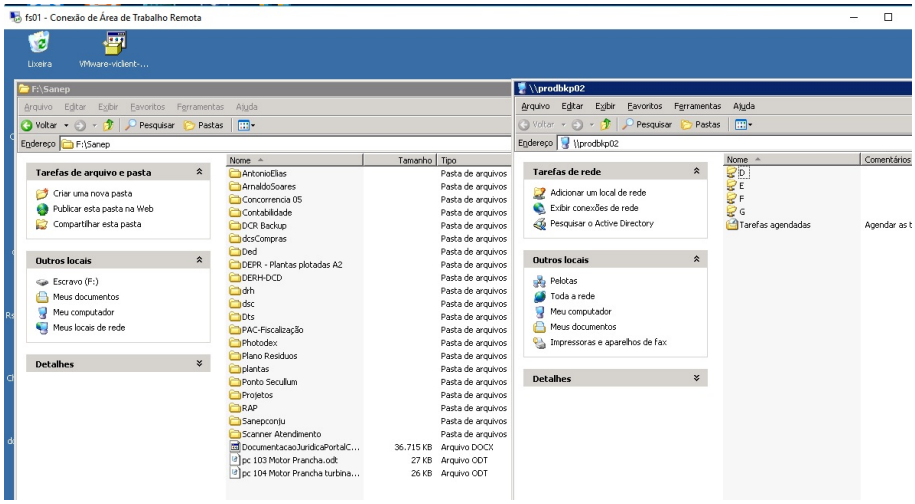

Figura 2. a) Servidor de Compartilhamento. b) Servidor de Backup

3. Princípios de Segurança

A segurança está relacionada à proteção das coisas que têm valor para uma organização ou pessoa. Isso inclui bens materiais, intelectuais, e nesse caso específico, informações e dados. O que quer que possa causar uma falha na proteção deve ser considerado uma ameaça à segurança. A quantidade de forma que ameaças podem ocorrer é vasta e dessa forma a segurança pode se tornar um problema difícil de ser solucionado.

Com isso é perceptível à importância de uma mão de obra e de uma rede que providenciem segurança para os dados empresariais e informações. Ainda nos princípios da segurança temos os pilares, segundo [Feleol 2009], são os elementos básicos para a sua estruturação. Sendo eles:

Privacidade ou Confidencialidade: Restrição de acesso, é a garantia de que a informação é somente acessível por pessoas autorizadas.

Integridade: Proteção contra adulteração ou perda. A política de segurança deve ser capaz de proteger a integridade das informações para evitar uso indevido das mesmas.

Disponibilidade: Impede a interrupção de um serviço. Se as informações necessárias ao andamento dos negócios da empresa não estiverem disponíveis, certamente a empresa perderá dinheiro. Assim, as informações devem estar disponíveis na hora certa para as pessoas certas.

4. Ferramenta de Backup

Não é novidade que fazer backup de dados é essencial para a segurança e continuidade das informações. Tão importante quanto a cópia, é o local onde ela é feita e a maneira como ela é executada. A quantidade de informação gerada hoje em dia por empresas cresce exponencialmente e, assim, torna-se relevante não só a necessidade de proteger, mas também a preocupação com os custos necessários para assegurar a continuidade dos negócios contra o risco da perda de informações. Devido a isto, são necessárias ferramentas de backup para o melhor controle, e segurança de que dados vão ser transferidos de forma correta sem causar problemas a parte.

4.1. ElkarBackup

O ElkarBackup [ElkarBackup 2017] é uma solução de backup de código aberto gratuita baseada em Rsync [Rsync 2017] / Rsnapshot [Rsnapshot 2017] e suas principais características são os backups centralizados, interface web intuitiva, backup de clientes Linux/Windows, recuperação instantânea, pré-scripts e pós-scripts.

4.1.1. Protocolo RSYNC

Rsync [Rsync 2017] (Remote Sync) é um utilitário para realizar cópias e sincronismo de arquivos (ou diretórios) localmente ou remotamente. Uma forma simples de fazer backups completos de grandes quantidades de arquivos, ou mesmo partições inteiras, mantendo uma única cópia atualizada de tudo em um HD externo ou num servidor remoto.

O Rsync sincroniza arquivos e diretórios localmente ou remotamente, fazendo uma cópia exata dos arquivos. Ele permite sincronizar o conteúdo de duas pastas, transferindo apenas as modificações. Ele não trabalha apenas comparando arquivo por arquivo, mas também comparando o conteúdo de cada um. Se apenas uma pequena parte do arquivo foi alterada, o rSync transferirá apenas ela, sem copiar novamente todo o arquivo.

Antes de transferir os dados, faz uma comparação do arquivo na origem e no destino. Os arquivos são quebrados em segmentos e os seus checksums são comparados. Os pedaços cujos checksums forem diferentes são transmitidos.

4.1.2. Rsnapshot

Rsnapshot [Rsnapshot 2017] é um utilitário de instantâneo de sistema de arquivos com base em Rsync, fáceis fazer instantâneos periódicos de máquinas locais e máquinas remotas em cima de ssh. O código faz uso extensivo de hardlinks sempre que possível, para reduzir significativamente o espaço em disco necessário.

Dependendo da sua configuração, é bem possível configurar em apenas alguns minutos. Os arquivos podem ser restaurados pelos usuários que os possuem, sem o usuário root se envolver.

Não há motivos para mudar, então, uma vez que está configurado, seus backups podem acontecer de forma íntegra, a não necessitar de interação humana. E porque o rsnapshot só mantém um número fixo (mas configurável) de instantâneos, a quantidade de espaço em disco usada não aumentará continuamente.

4.1.3. Funcionamento

O layout do ElkarBackup é bastante simples, de forma que ajude ao usuário a ter o controle íntegro da manutenção dos backups. Após a configuração do protocolo Rsync no host destino, a configuração nele se torna simples e de forma permanente, tendo a responsabilidade apenas de agendar o horário adequado, e a verificação dos logs se o backup foi realizado com sucesso.

Conforme a Figura 3 e 4 é possível ter acesso a ferramenta de forma clara e objetiva, com o usuário e permissões dada pelo administrador da rede. E a configuração dos backups também, analisando pela Figura 4 que depois de configurado o destino e a origem o trabalho é apenas executar o backup e a analisar os logs se tudo está ocorrendo de forma segura.

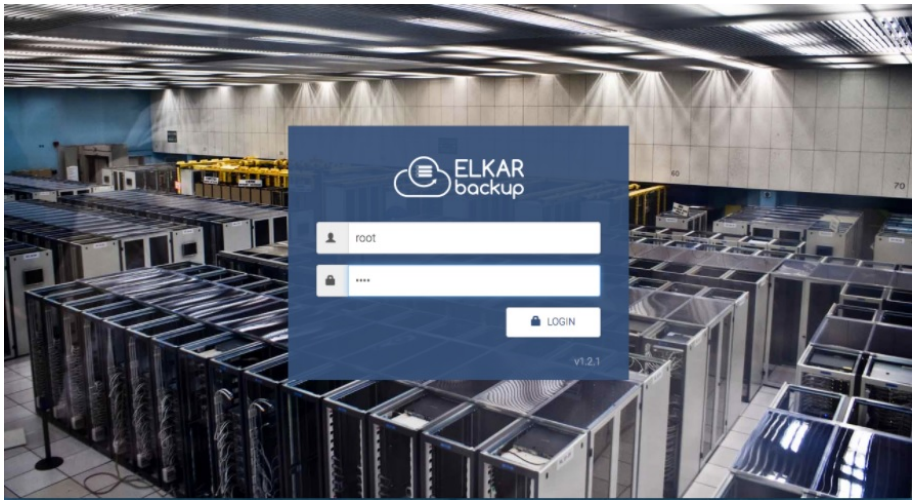

Figura 3. Plataforma do ElkarBackup

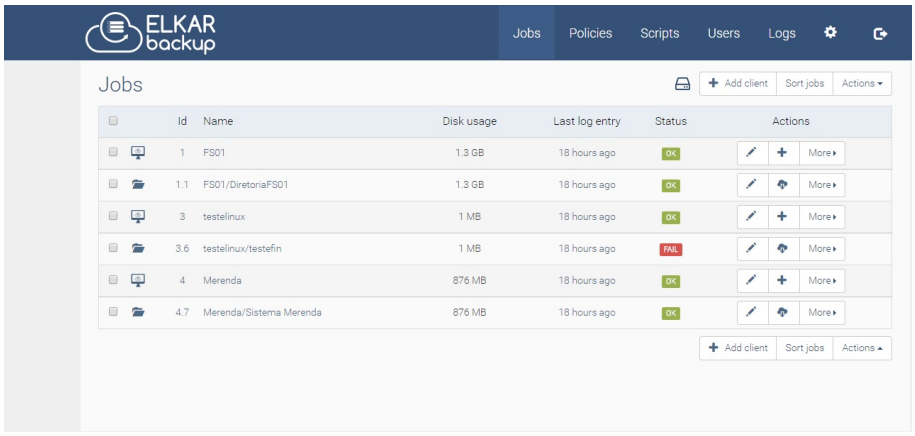

Figura 4. ElkarBackup em funcionamento

5. Ferramenta de Monitoramento

As ferramentas de monitoramento permitem que métricas sejam apresentadas de forma visual com gráficos e mapas. Informações de consumo de banda, CPU, memória, ou

tempo de consultas do banco de dados, podem ser rapidamente visualizadas, tanto com dados instantâneos como para dados históricos. Um bom sistema de monitoramento de redes permite a criação de alertas para eventos de anormalidade e também permitem correlacionar sintomas com itens de infraestrutura.

Outra característica de um bom sistema de monitoramento é que ele deve ser suficiente para atender as mais diversas equipes, ambientes e necessidades, de modo a evitar que múltiplas ferramentas sejam usadas, dificultando correlações e tornando o ambiente ainda mais complexo.

5.1. Nagios

O objetivo da ferramenta Nagios [Nagios 2017] é o de informar aos administradores rapidamente sobre condições questionáveis (warning) ou críticas (critical). O que é considerado ”questionável”ou ”crítico”é definido pelo administrador na configuração. Diferente das ferramentas de rede que mostram o tempo decorrido graficamente ou que registrem e meça o tráfego, o Nagios se utiliza de cores, como em um semáforo.

O Nagios monitora, desde que definido pelo administrador da rede, serviços como HTTP, SMTP, POP3 e NNTP. Esses serviços, em caso de imprevistos, precisam permanecer o menor tempo possível fora do ar, a fim de evitar o comprometimento de atividades essenciais à empresa. Desta forma, o Nagios permite o monitoramento da conectividade de maneira a perceber ou não a existência de um host ou serviço na rede.

Na Figura 05 é possível observar o Nagios em funcionamento, onde cada ponto (hosts ou serviço) estão sendo monitorados através do ping, se eles estão UP ou DOWN. O nagios neste estudo visa monitorar pontos críticos da infraestrutura da COINPEL como: servidores, switches gerenciáveis, roteadores e impressoras de rede.

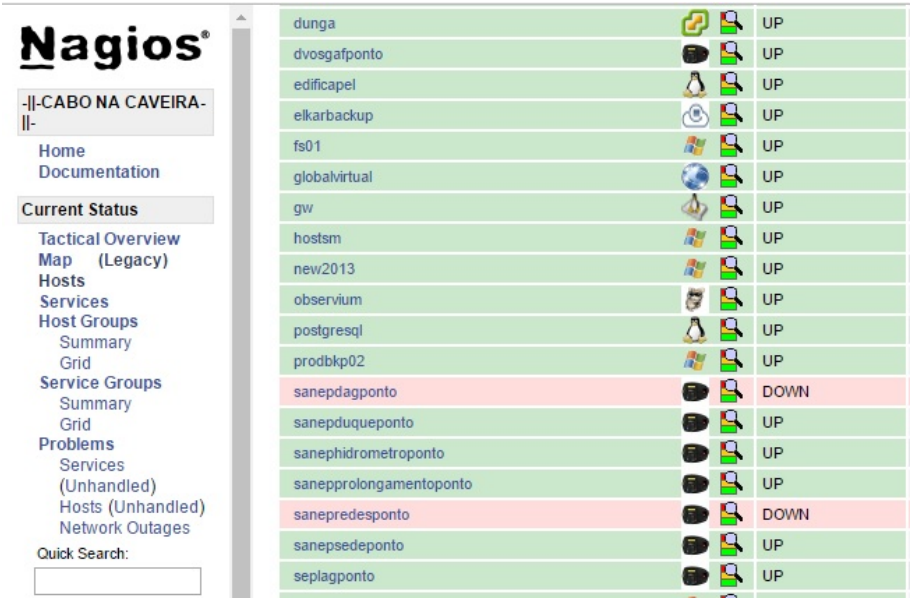

Figura 5. Monitoramento com o Nagios

6. Observium

O Observium [Observium 2017] é uma plataforma desenvolvida em PHP/MySQL, que permite a qualquer administrador observar/monitorizar toda a sua rede. Esta plataforma tem suporte para Linux, Windows entre outros. Em termos de gestão, o Observium oferece uma interface muito bem organizada, intuitiva e com bom desempenho. O Observium oferece várias funcionalidades que facilitam todo o processo de monitorização e alarmística. Esta plataforma está disponível em duas versões: Open Source e Profissional, mas a versão gratuita (open-source) oferece todas as funcionalidades básicas necessárias.

Na Figura 06 é possível observar o Observium em funcionamento, onde cada equipamento está sendo monitorado, e a ferramenta é capaz de informar o uso do hardware, largura de banda e etc. O observium neste estudo visa monitorar pontos críticos da infraestrutura da COINPEL como servidores.

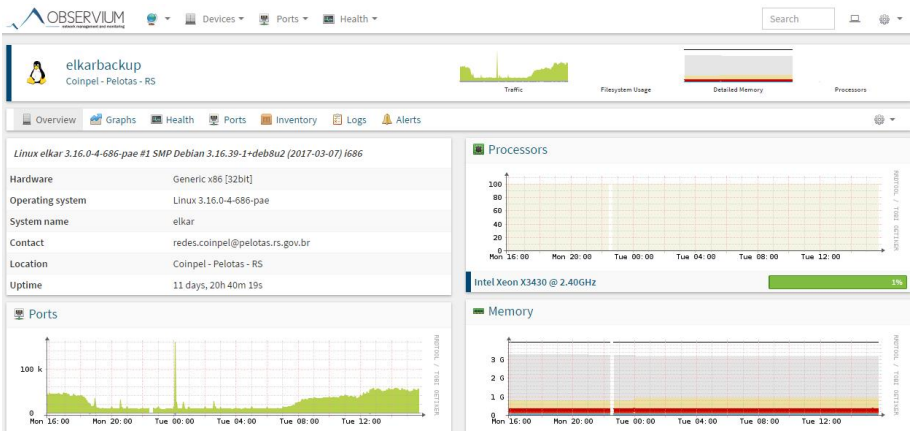

Figura 6. Monitoramento com o Observium

7. Testes Práticos

A partir desta seção serão abordados os testes práticos realizados na rede original no início dos estudos e compará-los com os testes após as modificações realizadas na rede.

7.1. IPerf

Segundo [Surhone 2009] o Iperf trata-se de software livre, do tipo cliente/servidor desenvolvido pelo National Laboratory for Applied Network Research (NLANR). Com ele pode-se testar e medir o throughput da rede, e é claro, também pode-se usá-lo como ferramenta de apoio para outros testes.

A aplicação JPerf apresenta uma interface gráfica baseada em Java visando simplificar a utililização de comandos no Iperf.

Para usar o Iperf/J-Perf basta inicializá-lo como servidor em um host, e como cliente em outro. O cliente passará a enviar tráfego TCP para o servidor por 10 segundos, e em seguida mostrará a quantidade dados transferida (MBytes) e a velocidade atingida (Mbits/s).

8. Teste de vazão da rede

Foi realizada uma bateria de testes nos principais pontos da rede da COINPEL, onde inicialmente o objetivo era a medição da vazão da rede. A ferramenta utilizada para os testes foi o JPERF. Os testes foram realizados com a rede em horários de alto fluxo na rede com exceção dos testes realizados diretamente nos conversores de fibra onde se eliminou a rede interna do prédio em questão.

8.1. Teste de vazão – Verificação de largura de banda disponibilizada pela Coinpel

O primeiro teste realizado foi conferir a largura de banda/link disponibilizado pela empresa. Realizando no mesmo cenário que na qual o backup é feito, ou seja, foi utilizado o I-Perf na escuta no servidor destino do backup, e no servidor de origem foi determinado o JPERF conferindo o link entre ambos. Tendo êxito conforme a Figura 7, o link atingiu 92,80Mbits por segundo.

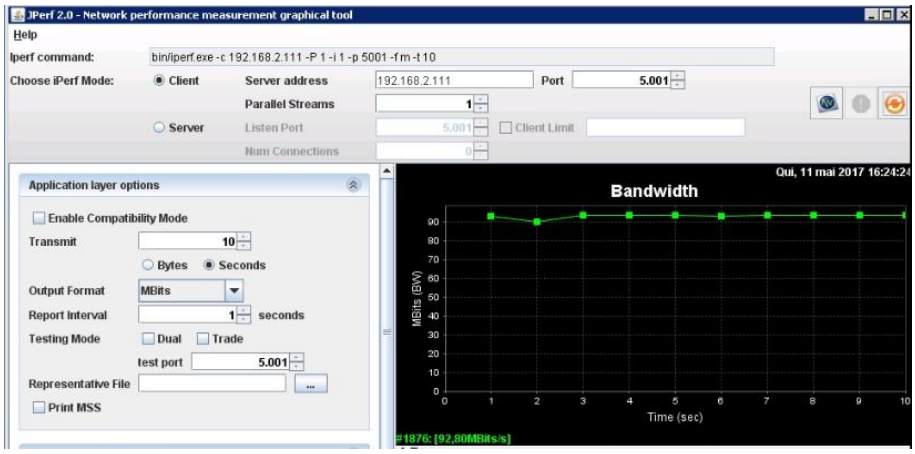

Figura 7. Largura de banda

8.2. Teste de vazão – Verificação da largura de banda no momento do backup atual

O teste foi realizado em um ponto crítico, onde o backup atual estava sendo realizado em horário de produção no setor "produção" ocasionando constantes reclamações de lentidão. Conforme Figura 8 podemos ver o motivo claro, segundo o teste de vazão com o JPERF, a largura de banda encontrava-se baixa com 26,10MBits por segundo.

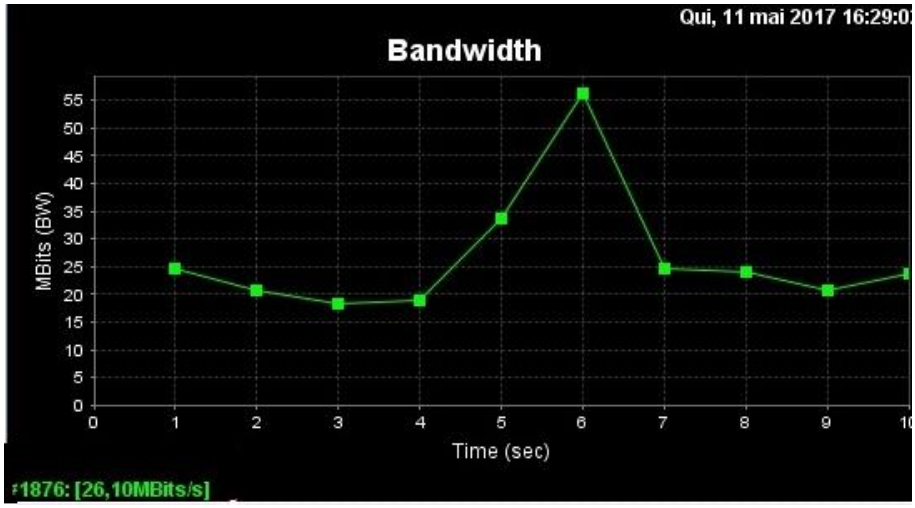

Figura 8. Backup atual

8.2.1. Analisando pelo Observium

Segundo teste realizado para comprovar as inúmeras reclamações de lentidão, foi monitorar a porta do tráfego de rede do switch principal de internet da empresa. Com a ferramenta de monitoramento Observium descrita acima, podemos ter a visualização completa a partir de gráficos, onde mostra o que o backup estava sendo realizado (09:00 as 16:00) consumindo 100 por cento do uso do link, 100MBits por segundo.

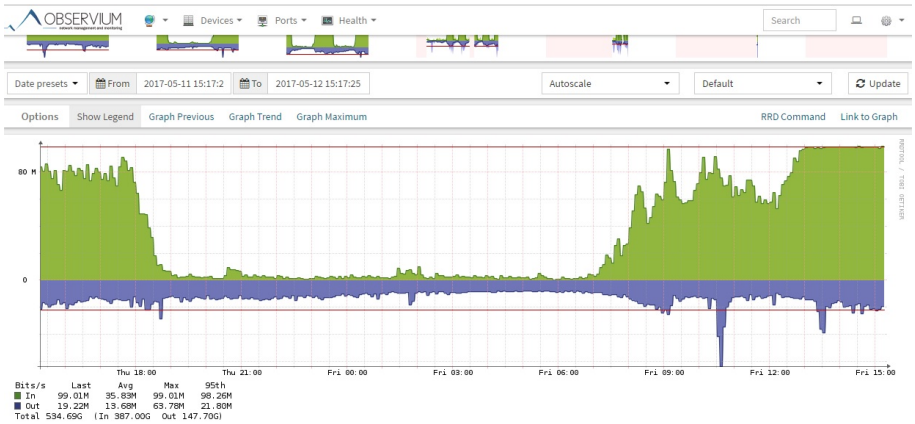

Figura 9. Porta do Switch Principal de Internet

8.3. Teste vazão - Implementação da solução de backup

A partir de agora os testes visam mostrar a melhora na infraestrutura da rede da COINPEL. Após a implementação da primeira solução de backup entre Matriz e Filiais, já foi possível observar uma melhora na taxa de vazão entre os prédios, que anteriormente era de 26,10 Mbit/s passou para 67,50,1 Mbit/s conforme ilustrado na Figura 10.

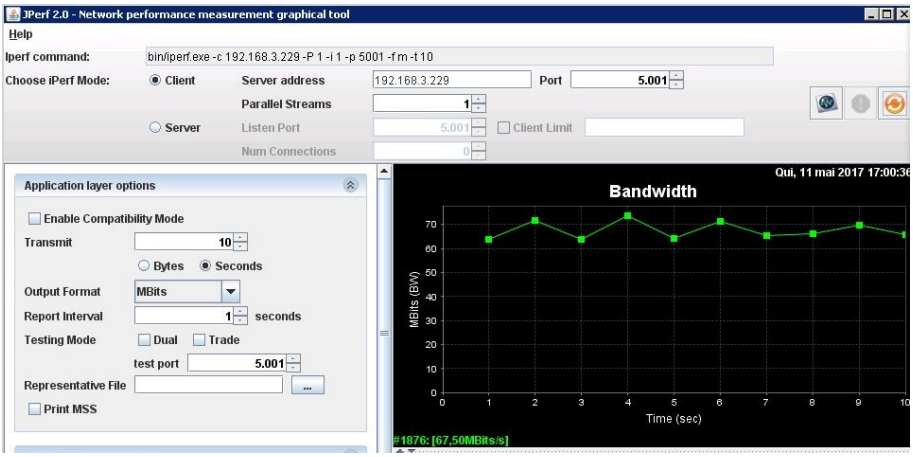

Figura 10. Rede segmentada

8.3.1. Rede Segmentada pelo Observium

Segundo testes de melhoria na infraestrutura da rede, embasados na ferramenta de monitoramento Observium, o Switch principal do link de internet estava sendo monitorado também e ao programar a ferramenta de backup para realização do mesmo fora do horário de produção, notamos o consumo da largura de banda, onde tivemos melhoria constante na rede.

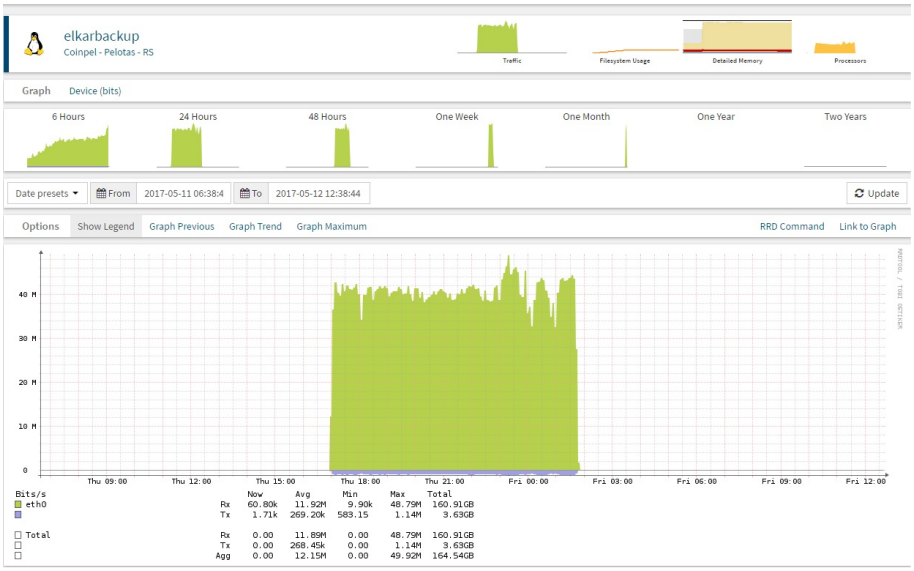

Figura 11. Rede segmentada - Observium

9. Hardware dos testes

Todos os testes realizados nesse artigo teve enfâse somente em um específico hardware, conforme Tabela 1 abaixo, mostra-se os recursos da máquina disponibilizada pela empresa.

Tabela 1. Recursos de hardware disponíveis

Recursos	Características
Disco	2TB
Memória RAM	16GB
Rede	100MB/s
processador	3.70 GHz

10. Resultado do testes

Após um estudo na infraestrutura da rede COINPEL, e a implementação da mesma, foram realizados testes em cima da rede atual com base na solução aplicada. E através dos testes obteve-se uma clareza de um melhor desempenho na rede, onde os resultados foram em cima de uma melhor perfomance na rede, contudo, as ferramentas aplicadas no decorrer do artigo tiveram sua importância para o bom manuseio do administrador e para aqueles que vão ter o controle dos backups.

10.1. Desempenho da Rede

Através da Figura 12 com base nos testes realizados com/sem a solução de backup, consegue-se visualizar de forma clara a melhoria na rede com a implementação da ferramenta de Backup, não causando mais lentidão perante ao de mais, e as reclamações diárias diminuiram.

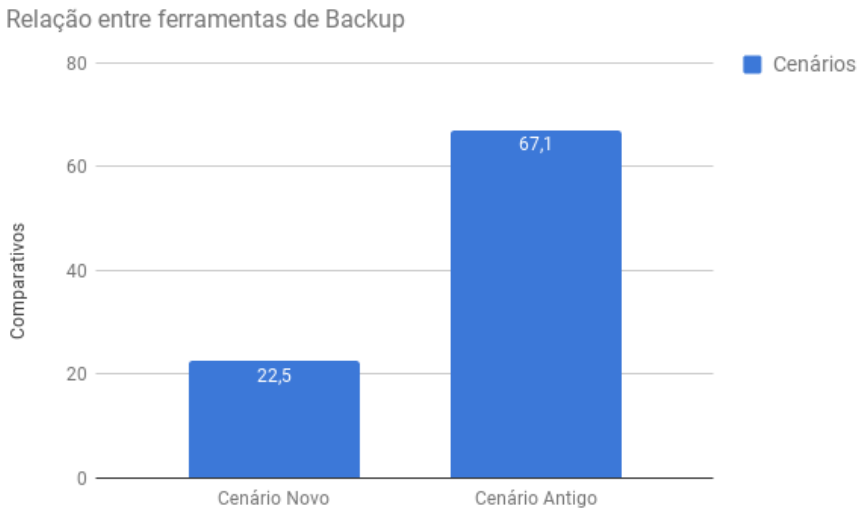

Figura 12. Gráfico apontando o resultado dos testes

11. Tempo na realização dos Backups

Baseado em horas, os resultados dos tempos entre os dois cenários (cenário atual/cenário novo) está claramente visto na Figura 13 abaixo, onde realizado backup do mesmo tamanho (75GB) em horário fora de produção. O cenário novo além de trazer melhor perfomance na rede, o tempo está bom baseado no cenário antigo.

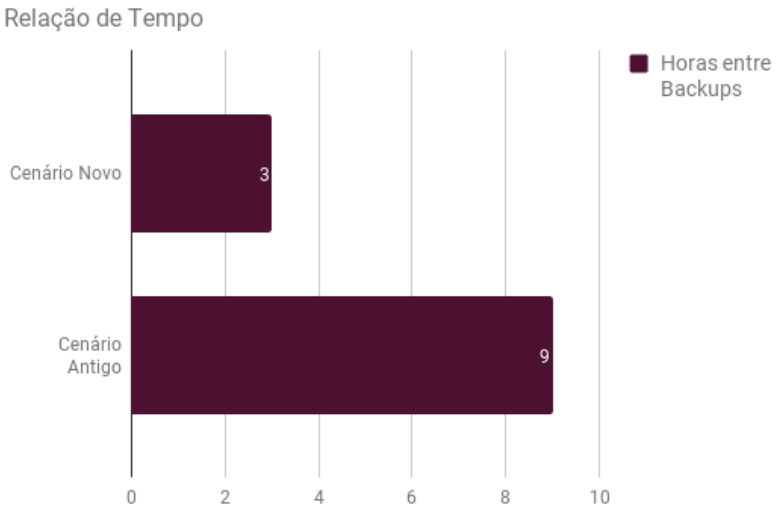

Figura 13. Tempo na realização dos Backups

12. Restauração dos Backups

Cenário Antigo: Baseado nas realizações inadequedas dos backups no cenário antigo, a restauração dos backups não existia. Ou melhor, os backups realizados ficavam disponibilizados em servidores de compartilhamento, onde usuário e colaborador tinham acesso a eles, caso precisasse dos dados ou informações. Podendo causar algum equívoco nos dados e ocasionar problemas com exclusão ou roubo de informações.

Cenário Novo: Conforme aplicação do cenário novo na empresa, os backups estão sendo salvos em storage com segurança total dos dados. Caso precisa-se dos dados teria que informar ao administrador da rede que disponibiliza o arquivo por completo. Baseando-se no tempo da restauração do backup, foram gerado testes de arquivos especificos de 10 GB, onde demorou-se em torno de 35 minutos (em horário de produção) para que os arquivos fossem disponibilizado.

13. Resultados e Conclusões

Foram muitas dificuldades, raciocínio, ideias, debates em grupo e muito estudo. Depois com a ideia amadurecida veio o planejamento, o desenvolvimento, os testes e enfim a tão almejadas conclusões. Conclui-se também que, através de nossa própria dificuldade na realização deste trabalho de tamanha envergadura e responsabilidade, sentimos o quanto este artigo será importante para os de mais.

Nota-se a grande importância das aplicações técnicas usadas ao decorrer do projeto para o dia a dia de um administrador de Redes e para futuras situações que reflitam a segurança de uma rede de computadores, porém não somente em ambiente empresarial, mas em qualquer rede que abrange técnicas abordadas, e suas polivalências. Ao decorrer do projeto e de sua aplicação é notável a sua importância, onde os valores morais e éticos de um profissional de Redes são colocados à prova em meio a responsabilidade sustentada durantes testes e, consequentemente, contato com informações de alto sigilo empresarial.

As técnicas empregadas neste artigo já demonstram uma melhora na performance do tráfego corporativo, comparadas ao cenário inicial em que eram latentes os efeitos de baixa performance em aplicações em vários pontos distintos da rede. A comprovação da melhora está visível nos testes práticos aplicados neste artigo. A origem deste projeto foi um marco inicial para a reestruturação da rede da COINPEL, onde muitas melhorias foram aplicadas ao longo deste período como documentação da rede, documentação das redes internas, aplicação de novas tecnologias (Solução em Backup), monitoramento dos hosts e principalmente melhora no tráfego das aplicações da rede. Posteriormente novos estudos serão realizados para manter a infraestrutura da COINPEL em constante crescimento tecnológico.

Referências

ElkarBackup (2017). Elkarbackup. http://www.elkarbackup.org. Accessed: 2017-05-27.

Feleol, A. E. (2009). TrÊs pilares de segurança - guia pratico. In Feleol, A., editor, *Segurança da Informação*. Editora Meridional LTDA.

Nagios (2017). Nagios. https://www.nagios.org/. Accessed: 2017-05-13.

Observium (2017). Observium. http://www.observium.org/. Accessed: 2017-06-14.

Rsnapshot (2017). Backup rsnapshot. http://www.dicas-l.com.br/arquivo/snapshot. Accessed: 2017-05-14.

Rsync (2017). Protocolo rsync. http://www.hardware.com.br/dicas/usando-rsync.html. Accessed: 2017-05-13.

Surhone, L. (2009). Iperf. In Susiam, M., editor, *Segurança da Informação*. Editora Meridional LTDA.