INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA
E TECNOLOGIA DO AMAPÁ – IFAP
CAMPUS MACAPÁ
CURSO SUPERIOR DE TECNOLOGIA EM REDES DE COMPUTADORES

ADSON JAIRO DE LIMA ROSA
ALISON JORDAN DE LIMA ROSA

ESTUDO DE CASO NA IMPLEMENTAÇÃO DE SERVIÇOS DE GERENCIAMENTO E MONITORAMENTO EM UMA REDE DE PEQUENO PORTE

MACAPÁ - AP
2020

ADSON JAIRO DE LIMA ROSA
ALISON JORDAN DE LIMA ROSA

ESTUDO DE CASO NA IMPLEMENTAÇÃO DE SERVIÇOS DE GERENCIAMENTO E MONITORAMENTO EM UMA REDE DE PEQUENO PORTE

Trabalho de conclusão de curso apresentado ao curso Superior de Tecnologia em Redes de Computadores, do Instituto de Educação, Ciência e Tecnologia do Amapá – IFAP, como requisito avaliativo para obtenção de título de Tecnólogo em Redes de Computadores

Orientador: Prof. Dr. Klenilmar Lopes Dias

MACAPÁ – AP
2020

Biblioteca Institucional - IFAP
Dados Internacionais de Catalogação na Publicação (CIP)

R788e Rosa, Adson Jairo de Lima
Estudo de Caso na implementação de serviços de gerenciamento e monitoramento em uma rede de pequeno porte / Adson Jairo de Lima Rosa, Alison Jordan de Lima Rosa. - Macapá, 2020.
52 f.: il.

Trabalho de Conclusão de Curso (Graduação) -- Instituto Federal de Educação, Ciência e Tecnologia do Amapá, Campus Macapá, Curso de Tecnologia em Redes de Computadores, 2020.

Orientador: Prof. Dr. Klenilmar Lopes Dias.

1. Gerenciamento de Redes de Computadores. 2. Serviços de Redes de Computadores. I. Rosa, Alison Jordan de Lima. I. Dias, Prof. Dr. Klenilmar Lopes, orient. II. Título.

Elaborada pelo Sistema de Geração Automática de Ficha Catalográfica do IFAP
com os dados fornecidos pelo(a) autor(a).

ADSON JAIRO DE LIMA ROSA
ALISON JORDAN DE LIMA ROSA

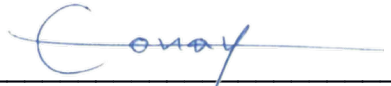
ESTUDO DE CASO NA IMPLEMENTAÇÃO DE SERVIÇOS DE GERENCIAMENTO E MONITORAMENTO EM REDES DE PEQUENO PORTE

Trabalho de conclusão de curso apresentado ao curso Superior de Tecnologia em Redes de Computadores, do Instituto de Educação, Ciência e Tecnologia do Amapá – IFAP, como requisito avaliativo para obtenção de título de Tecnólogo em Redes de Computadores

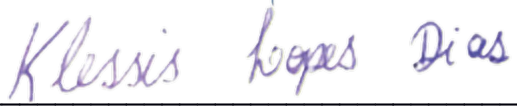
Orientador: Prof. Dr. Klenilmar Lopes Dias

BANCA EXAMINADORA

Prof. Dr. Klenilmar Lopes Dias



Prof. Esp. Eonay Barbosa Gurjão



Prof. Me. Klessis Lopes Dias

Aprovado em : 18 / 12 / 2020

Nota: 10

À nossa família.

AGRADECIMENTOS

A Deus pelas oportunidades e bênçãos a nós concedidos.
A nossa mãe por estar sempre nos apoiando.
A nossa irmã que sempre esteve do nosso lado.
Ao nosso pai que com que sempre pudemos contar.
A todos os professores do Instituto Federal do Amapá pelo esforço em nos passar os conhecimentos necessários para atuar nessa profissão.
Ao nosso professor orientador pelo seu apoio, orientação e ideias que fizeram desta uma experiência inspiradora para nós.
Aos colegas de trabalho na Polícia Rodoviária Federal que nos permitiram ganhar experiência de trabalho que será muito importante no futuro.
O nosso muito obrigado a todos.

RESUMO

Tendo em vista que o uso das redes de computadores vem crescendo ano após ano, pesquisa-se sobre aplicações de gerenciamento de redes de computadores focadas nas redes de pequeno porte, a fim de elencar as melhores aplicações que possam ser adotadas em projetos de redes para Micro e Pequenas Empresas no ano de 2020. Para tanto, é necessário identificar quais sãos os pontos importantes a serem observados na gerência da rede de uma empresa de pequeno porte, catalogar quais aplicações atendem aos requisitos antes identificados, implementar as aplicações selecionadas em um ambiente real de produção e por fim avaliar os resultados obtidos na implementação. Realiza-se, então, uma pesquisa básica estratégica com objetivos descritivo e exploratório, através do método hipotético dedutivo, adotando uma abordagem qualitativa dos dados coletados, utilizando procedimentos bibliográficos, documental e um estudo de caso da Superintendência da Polícia Rodoviária Federal no Estado do Amapá. Diante disso, após o uso de soluções como o ZABBIX verificou-se que os resultados confirmaram à hipótese levantada, o que impõe a constatação de que as Micro e Pequenas Empresas podem adotar o ZABBIX como uma aplicação viável e de uso livre para gerenciamento de redes de computadores melhorando o controle interno e monitoramento tanto da rede lógica quanto do hardware dos hosts. Além disso a solução permite criar mapas detalhados da rede local e melhorias no tempo de resposta a incidentes na rede gerando assim um aumento no desempenho e produtividade de uma MPE.

Palavras-chave: Gerenciamento. Redes de Computadores. MPE. Aplicações. Projeto de Redes.

ABSTRACT

Given that the use of computer networks has been growing year after year, research is carried out on the management of computer networks focused on small networks, in order to list the best applications for network management that can be adopted in network projects for Micro and Small Enterprises in 2020. Therefore, it is necessary to identify and detail which are the important points to be observed in the management of a network of a small company, catalog which applications meet the requirements previously identified, implement the selected applications in a real production environment and finally evaluate the results obtained in the implementation. A basic strategic research with descriptive and exploratory objectives is then carried out, through the deductive hypothetical method, adopting a qualitative approach to the collected data, using bibliographic and documental procedures and a case study of the Superintendência da Polícia Rodoviária Federal. Therefore, after the use of solutions such as ZABBIX it is verified that the resultados has confirmed our hypothesis, which imposes the verification that Micro and Small Companies can adopt ZABBIX as a viable application and free use for computer network management improving the internal control and monitoring of both the logical network and the hardware of hosts. In addition, the solution allowed the creation of detailed maps of the local network improving the response time to incidents in the network and in which sector, thus generating an increase in the productivity and process performance of an MPE.

Keywords: Management. Computer Networks. MPE. Applications. Network Design.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
ARP	Address Resolution Protocol
COBIT	Control Objectives for Information and Related Technologies
DNS	Domain Name System
EIA	Electronic Industries Alliance
FTP	File Transfer Protocol
GPL	General Public Licence
ICMP	Internet Control Message Protocol
IEC	International Electrotechnical Commission
IP	Internet Protocol
ISACA	Information Systems Audit and Control Association
ISO	International Organization of Standardization
ITGI	IT Governance Institute
LAN	Local Area Networks
MAC	Medium Access Control
MIB	Management Information Base
MPE	Micro e Pequenas Empresas
NBR	Norma Brasileira Reguladora
OSI	Open Systems Interconnection
PC	Personal Computer
RDP	Remote Desktop Protocol
SEBRAE	Serviço Brasileiro de Apoio às Micro e Pequenas Empresas
SNMP	Simple Network Management Protocol
SPRF	Superintendência da Polícia Rodoviária Federal
TI	Tecnologia da Informação
TIA	Telecommunications Industry Association
TICS	Tecnologia da Informação e Comunicação
USB	Universal Serial Bus
VAL IT	value from IT investments
VPN	Virtual Private Network
WAN	Wide Area Network

SUMÁRIO

1 INTRODUÇÃO

No artigo publicado no portal de notícias G1 (2015), o analista sênior de Tecnologia da Informação (TI) da consultoria Frost & Sullivan, Bruno Tasco, diz que “Os serviços de monitoramento são importantes para que os gestores de TI tenham indicadores de como está a performance da rede e o seu tráfego para tomar decisões”.

Tal afirmação revela um dos principais desafios que as empresas de todo o mundo enfrentam na atualidade, haja visto que com o crescente aumento do uso das redes de internet, como aponta Luciano Ribeiro (2019), ao divulga a pesquisa realizada pela TIC Domicílios que “70% dos brasileiros estão conectados à internet”, as empresas precisam informatizar seus serviços e produtos além de mantê-los em pleno funcionamento vinte quatro horas por dia, sendo, portanto, imprescindível o monitoramento constante desses sistemas.

As Grandes Corporações já vêm implementando políticas de gerenciamento de rede em suas infraestruturas de TI, porém as Micro e Pequenas Empresas (MPE), que em 2019 eram cerca de 6,33 milhões de estabelecimentos no Brasil, segundo dados do Serviço Brasileiro de Apoio às Micro e Pequenas Empresas (SEBRAE), anda possuem um grande déficit nesta área em relação às empresas de grande porte, seja por falta de capital ou por falta de profissionais de TI que detenham conhecimento especializado em gerenciamento de redes.

Nestas circunstâncias, percebe-se a necessidade de se elaborar projetos de redes para MPE que contenham mecanismos de gerenciamento de rede de baixo custo e fácil controle por parte dos profissionais de TI.

Portanto questiona-se: quais são as aplicações voltadas ao gerenciamento de rede ideais a serem adotadas em projeto de redes para MPE no ano de 2020?

Dito isso, o objetivo geral da presente pesquisa é elencar as melhores aplicações voltadas ao gerenciamento de redes que possam ser adotadas em projetos de redes para Micro e Pequenas Empresas no ano de 2020.

Para tanto, foram pontuados os seguintes objetivos específicos: identificar quais são os pontos importantes a serem observados na gerência da rede de uma MPE, catalogar quais aplicações atendem aos requisitos antes identificados, implementar as aplicações selecionadas em um ambiente real de produção e por fim avaliar os resultados obtidos na implementação.

Parte-se da hipótese de que o Zabbix é a melhor ferramenta de gerenciamento de redes de computadores disponível atualmente no mercado pois, além de ser open-source, companhias ao redor do mundo demonstram grande confiança nas suas soluções e avançada performance. Entre seus usuários estão instituições e empresas de diferentes tamanhos que operam na indústria de finanças e seguros, Tecnologia da Informação e Comunicação (TICS), saúde, alimentação, educação, varejo e muitos outros setores da economia. Podemos citar como exemplo de cliente as gigantes Dell e Renner.

Para provar tal hipótese é necessário realizar uma pesquisa básica estratégica com objetivos descritivo e exploratório, através do método hipotético dedutivo, adotando uma abordagem qualitativa dos dados coletados, utilizando procedimentos bibliográficos, documental e um estudo de caso da Superintendência da Polícia Rodoviária Federal no Estado do Amapá (SPRF-AP).

No primeiro capítulo, destaca-se a importância da administração de redes de computadores para as empresas, pontuando-se os principais trabalhos desempenhados pelos administradores de rede, além de explicar o conceito de Governança de TI descrevendo seus principais modelos.

No segundo capítulo, aponta-se a crescente relevância do gerenciamento de rede para as empresas bem como as dificuldades em se aplicar esse gerenciamento, detalhando de forma mais específica o monitoramento de redes com suas várias ferramentas.

No terceiro capítulo foram analisadas três aplicações de monitoramento de rede com base nos critérios definidos que visam o melhor proveito por parte das MPE.

No quarto capítulo, descreve-se a estrutura da rede da Superintendência Regional da Polícia Rodoviária Federal no Amapá, sendo este o local onde foi realizado o estudo de caso, assim como os processos de instalação da aplicação melhor avaliada no capítulo anterior.

Ao final, conclui-se que os objetivos foram atingidos e a hipótese antes apresentada para solução do problema foi confirmada, indicando que as MPE podem adotar o ZABBIX como uma aplicação viável e de uso livre para gerenciamento de redes de computadores, garantindo assim uma redução significativa dos custos com equipamentos e melhorias no tempo de resposta a incidentes na rede e consequentemente permitindo um aumento da produtividade da empresa.

2 ADMINISTRAÇÃO DE REDES

A evolução das redes de computadores e o desenvolvimento de aplicações e serviços de redes gerou uma dependência primordial das empresas que tem como negócio o uso destas tecnologias. O ambiente competitivo do mercado atual se mostrou favorável a empresa que possui os melhores requisitos tecnológicos dentro de sua faixa de atuação, porém não basta somente se ter tais recursos, pois não saber como administrá-los e gerenciá-los de forma correta, acaba por gerar um desperdício de capital e por consequência a falência do negócio.

Como explicou Vumo (2017), no documento que estrutura um curso de Administração de Rede pela Universidade Virtual Africana, os administradores de rede surgiram pelas necessidades das empresas em gerenciar e manter seus crescentes parques tecnológicos em pleno funcionamento. O trabalho de um administrador de redes é o mesmo que de um administrador de empresa, porém ao invés de gerenciar pessoas na execução de tarefas, seu trabalho e gerenciar máquinas na execução de serviços.

Vumo ainda definiu dois tipos de comportamento que um administrador de rede pode adotar, sendo estes uma postura Pró-Ativa, onde o administrador realiza revisões periódicas do funcionamento da rede, coletando informações constantemente dos equipamentos monitorados. Tal postura requer um investimento maior em aplicações que monitoram a rede, normalmente estas aplicações são caras e de difícil implementação e análise dos seus dados.

Postura Reativa o administrador apaga incêndios, sendo, portanto, responsável por solucionar problemas que geralmente não são de sua competência, como dar suporte ao usuário, realizar manutenção em notebooks e PC’s, esclarecer dúvidas recorrentes etc. Esse profissional está mais presente em pequenas empresas que não possuem o capital necessário para implantação de sistemas de monitoramento em tempo real para que assim o administrador possa antever problemas na rede.

Dentre as atividades que um administrador de rede tem de executar, as principais são, gerir as contas dos utilizadores, gerenciar os servidores, gerenciar a rede de computadores, fazer backups, gerenciar os sistemas da empresa, realizar auditorias e manter atualizado a documentação da rede.

2.1 Governança de TI

Segundo Fábio Teles (2017), governança de TI é uma extensão da Governança Corporativa, pois trata da adoção de processos, regras e ações padrões na manutenção, implementação e monitoramento de todo o parque tecnológico de uma empresa, sendo que estes métodos devem estar alinhados com os objetivos e diretrizes do negócio.

Tais regras e processos devem constar no plano de governança de TI e tem de ser seguido por todos os funcionários de uma empresa, a fim de garantir a segurança da informação, a disponibilidade dos sistemas, a durabilidade dos serviços para a manutenção do negócio.

Ao longo dos anos foram desenvolvidos vários modelos de Governança de TI que podem ser adotados de acordo com a necessidade de cada corporação, portanto foi necessário a essa pesquisa realizar uma descrição superficial de cada um, pois são esses modelos que formam a base da Administração e Gerenciamento de Redes de Computadores.

2.2. Modelo de Governança de TI

2.2.1 COBIT5a

O COBIT5 nada mais é do que um modelo de Governança de TI, desenvolvido pela ideia de gerar valor a uma empresa por meio do seu parque tecnológico, adotando uma visão holística de toda a organização, para que assim possa atuar de ponta a ponta onde houver uso da TI, alinhados com os interesses da empresa (ISACA, 2012)

O modelo de COBIT5 se baseia em cinco princípios básicos segundo a Associação de Auditoria e Controle de Sistemas de Informação (ISACA) (2012), sendo estes o princípio da Atender às Necessidades das Partes Interessadas, visando gerar valor para as partes interessadas que administram a organização, o princípio de Cobrir a Organização de Ponta à Ponta, considerando a TI como um ativo a ser utilizado em toda a organização, Aplicar um Modo único de Integração, servindo como um modelo único para a governança corporativa e a de TI, Permite uma Abordagem Holística, definindo um conjunto de habilitadores que devem ser utilizados em toda a

organização, e por fim Distinguir a Governança da Gestão, adotando plano diferenciados para cada função.

2.2.2 Norma ISO/IEC 38500

Segundo explicação de Nascimento (2009) no site Portal GSTI, a norma ISO/IEC 38500 está fundada em seis princípios básicos que direcionam a Governança de TI da empresa que adota este modelo, sendo estes a:

- Responsabilidade - todos os integrantes da empresa devem aceitar a responsabilidade de gerir os equipamentos de TI;
- Estratégia - a estratégia de negócio da empresa é sustentada pela capacidade tecnológica que possui, sendo, portanto, necessário manter atualizada e funcional;
- Aquisição - a aquisição de equipamentos ou serviços de TI deve levar em conta seus benefícios, riscos, custos e as oportunidades cruciais que garantam o futuro da organização, visando a produtividade ao invés de comodidade;
- Desempenho - a TI deve estar alinhada com os objetivos de negócio da empresa, visando dar suporte contínuo aos processos e as pessoas presentes na empresa, sendo, portanto, necessário adotar meios de se avaliar seu desempenho;
- Conformidade - a TI deve ter uma postura transparente perante a organização, aos seus funcionários e clientes, a fim de garantir o correto cumprimento das leis impostos pelas agências de controle;
- Comportamento humano - sendo necessário analisar suas necessidades ao longo do processo de desenvolvimento da organização, pois o quesito humano é inseparável do uso e aplicação da TI.

Com claros princípios, percebe-se a importância do papel que as pessoas desempenham na governança de TI de uma organização, pois são elas que dão a justificativa para empresa investir em seu parque tecnológico, haja visto que os equipamentos só terão valor se forem bem utilizados por pessoas competentes, atestando assim sua importância na organização.

2.2.3 VAL IT

Como relata Abreu e Fernandes (2012, p.227), no seu livro Implantando a Governança de TI, Val IT é um modelo que surgiu da necessidade de demonstrar aos empresários o retorno que o investimento em TI traz para seu negócio. Este modelo foi encabeçado pelo IT Governance Institute (ITGI) que passou a disponibilizá-lo para uso da comunidade de TI em 2006 e 2008 na sua segunda edição.

Continua Abreu e Fernandes (2012), onde explica que os objetivos desse modelo é auxiliar a gerência empresarial em obter o maior retorno nos investimentos em TI, suprimindo ao máximo os custos e riscos por meio de diretrizes, processos e práticas que subsidiem a gestão executiva em relação aos investimentos em TI.

O Val IT pode ser tratado como um complemento ao COBIT, uma vez que este trata das implicações decorrentes do investimento de TI e o COBIT trata da execução propriamente dita desses investimentos.

2.2.4 RISK IT

De acordo com Abreu e Fernandes (2012, p. 237), o modelo Risk IT foi desenvolvido com o intuito de auxiliar no gerenciamento de risco em TI, contando com a participação de vários especialistas e servindo como complemento ao COBIT.

Os objetivos desse modelo são voltados a dar suporte a empresa fornecendo-a informações sobre a extensão dos riscos e sua tolerância e apetite em face disso, visando integrar o Gerenciamento de Risco em TI com o Sistema de Gerenciamento de Risco da Organização para que a mesma possa entender os risco e como lidar com eles na administração do negócio (ABREU; FERNANDES, 2012).

O modelo Risk TI atende a necessidade encontrada por muitos profissionais da área de TI de demonstrar aos administradores de uma empresa, na qual trabalham, a importância de se investir na área de TI, pois ao adotar este modelo de Governança de TI todo a parte tecnológica da empresa fica sendo encarada como área estratégica, crucial para o alcançar dos objetivos do negócio, sendo, portanto, impossível de se ignorar pelo Sistema de Gerenciamento da Organização.

2.2.5 DevOps

DevOps não é um modelo, padrão ou tecnologia desenvolvida para a venda no mercado, mas sim um “movimento” ou “cultura” que vem sendo adotada pelas equipes de TI das empresas ao redor do mundo.

Segundo o que Danilo Sato diz no seu livro DevOps na Prática ([201-], p. 06), DevOps visa criar uma cultura de colaboração entre as divisões de Desenvolvimento e Operação de sistemas com intuito de solucionar o gargalo entre a fase de criação e otimização de software e a fase de implementação e manutenção no ambiente de produção, diminuindo o risco de incidentes e aumentando a robustez e a disponibilidade do serviço para os clientes.

Como o objetivo é a rapidez na entrega de atualizações ao ambiente de produção, o DevOps trabalha muito com a automatização dos processos que compõem a cadeia de produção do software, como os processos de testes, compilação de código e configurações, garantindo uma dinâmica melhor de trabalho.

Fica claro que a adoção do DevOps não está restrita a desenvolvimento de sistemas e software, mas também a todo o gerenciamento do parque tecnológico de uma empresa, desde a manutenção, configuração e implantação até a segurança, conexão e disponibilidade tanto para o administrador quanto para os clientes. Seu alto rendimento se mostra claro quando se é conhecido que as Big Tech, como a Amazon, Google e Facebook, fazem uso dessa cultura.

3 GERENCIAMENTO E MONITORAMENTO DE REDES

Na sociedade da informação o acesso rápido, constante e seguro ao principal ativo deste século, a informação, tornou-se um dos pilares que a sustentam. Tendo isso em mente Filho (2012), comenta, em sua monografia, sobre a demanda que as empresas e os negócios têm em relação às redes de telecomunicações, gerando uma dependência maior da infraestrutura tecnológica que precisa evoluir constantemente no intuito de dar o suporte necessário as várias tecnologias que vem surgindo na modernidade.

Neste contexto a gerência e o controle de tráfego da rede interna ganha relevância pontual para as organizações que buscam o aumento do desempenho de suas redes, principalmente para aquelas que têm negócios atrelados ao uso das redes de telecomunicações, como provedoras de internet, e-commerces, prestadores de serviços web entre outras

A International Organization for Standards (ISO) define cinco diferentes divisões chaves no gerenciamento de rede, sendo estas o gerenciamento de falhas, de configuração, de segurança, de performance e de contabilização.

Alves ([1992 ou 1994], p. 287) no seu livro Comunicação de Dados, já alertava sobre a importância de se adotar mecanismo eficientes para a gerência das redes de computadores nos ambientes corporativos, pois a informação gerada só ganha importância quando esta pode ser incrementada, manipulada e compartilhada, sendo imprescindível para isso uma rede em pleno funcionamento com os sistemas disponíveis o tempo todo. Como falhas não são impossíveis de ocorrer, cabe aos gerentes de rede utilizar-se de instrumentos de detecção e correção de falhas de forma eficiente que os permita diminuir ou inibir prejuízos aos negócios de empresas ou de órgãos públicos.

Continua Alves ([1992 ou 1994], p. 288), ao relatar que a dificuldade de gerenciar a rede vem crescendo significativamente nos últimos anos, uma vez que a heterogeneidade de produtos é muito grande. Isso sem levar em conta a diversidade de ambientes e a necessidade cada vez maior de que estes ambientes estejam interconectados. Portanto, a gerência de rede deve abranger não somente as considerações pertinentes ao ambiente local como também de ambientes remotos a estes.

Nesse aspecto, o autor constatou a importância e a relevância crescente da gerência das redes de computadores, tendo em vista a multiplicidade de ambientes e sistemas, a interação e interconexão entre esses ambientes, onde o administrador de rede tem de, não só aplicar mecanismo de gerência na sua rede local, como também em ambientes remotos.

Cabe ressaltar que ao se falar de gerência de rede, o administrador não deve se atentar apenas em seus aspectos operacionais técnicos, mas sim em todo um escopo abrangente e que vai de acordo com o modelo de implantação da rede. Dentre estes aspectos que podem ser observados, se encontram o atendimento ao usuário, organização das tarefas, controle de acesso à rede, disponibilidade e performance, documentação de configuração, gerência de mudanças, planejamento de capacidade, auxílio ao usuário, gerência de problemas, controle de inventário entre outros.

Como ressalta Sousa (2013, p. 305) no seu livro Projeto e Implementação de Redes, diz “o gerenciamento de rede é necessário para que haja seu controle proativo, detectando, por exemplo, problemas tão logo ocorram”. Como problemas no mundo real são inevitáveis é imprescindível o gerenciamento dos equipamentos em vista de detectar imediatamente gargalos na rede, falhas de segurança, erros de tráfego etc.

Em face destes problemas, a Internet Engineering Task Force (IETF) e a ISO desenvolveram os protocolos SNMP (Simple Network Management Protocol) e o ICMP (Internet Control Message Protocol), combinado em uma estrutura de gerenciamento chamado de Framework no qual agentes são instalados nos equipamentos a serem gerenciados com o objetivo de fornecer uma base de dados chamada MIB (Management Information Base) ao gerenciador central de rede que cria estruturas de informações e suas especificações e emite alertas caso ocorra alguma falha (SOUSA, 2013).

Uma ferramenta que auxilia no gerenciamento remoto são as Virtual Private Networks (VPN) que segundo Sousa (2013, p. 301) as VPN’s são canais de conexão entre duas redes locais distantes uma da outra, pela internet de modo a simular uma rede privada utilizando-se de criptografia que só entende o transmissor e receptor.

Com o uso desta tecnologia os administradores de rede podem acessar remotamente, por meio da rede pública de forma segura equipamentos físicos presentes nas redes corporativos como switches, roteadores, servidores e demais dispositivos, garantindo assim um controle e gerenciamento em tempo hábil, haja visto

que qualquer problema que sujar na rede, o administrador aplicará as devidas correções independente do horário ou local a qual esteja.

3.1 Monitoramento

O monitoramento é a principal forma de termos visibilidade nos sistemas que administramos. É o processo de observação de informações sobre o estado das coisas para uso na tomada de decisões. O objetivo operacional do monitoramento é detectar os precursores de interrupções para que possam ser corrigidos antes que se tornem interrupções reais, coletar informações que ajudem na tomada de decisões no futuro e, é claro, detectar problemas no ambiente de produção. O sistema de monitoramento ideal torna a equipe de operações omnisciente e omnipresente. Há um ditado no mundo dos negócios que, se não se pode medir, não se pode gerir. Isto também se aplica à administração de sistemas. Na verdade, o objetivo do monitoramento é tornar nossos sistemas observáveis. O monitoramento é um componente importante para fornecer um serviço confiável e profissional (LIMONCELLI; HOGAN; CHALUP, 2017, p. 671).

Limoncelli, Hogan e Chalup continuam ao afirmar que o monitoramento é ainda mais crítico onde é necessário um tempo de atividade elevado, como por exemplo, com sites de comércio eletrônico e serviços de emergência. No entanto, também é importante nas aplicações empresariais diárias onde se espera que estejam disponíveis de segunda a sexta-feira durante o horário comercial.(The Practice of System and Network Administration, 2017, p. 672).

3.1.1 Tipos de Monitoramento

Existem dois tipos de monitoramento: Histórico e de Tempo Real. O monitoramento Histórico armazena dados que serão utilizados posteriormente para análise. Já o monitoramento em Tempo Real gera alertas de incidentes que são informados ao administrador de sistemas.

O monitoramento histórico é usado para registrar o tempo de atividade, uso e desempenho a longo prazo. Contém dois componentes: a coleta dos dados e a visualização dos dados. Os dados de utilização são usados para o planejamento de capacidade. Por exemplo, o usuário pode ver um gráfico de utilização da largura de

banda recolhida, no último ano, de um link de Internet.(LIMONCELLI; HOGAN; CHALUP, 2017, p. 672).

O monitoramento em tempo real alerta o administrador de sistema de uma falha assim que ela acontece. Tem dois componentes básicos: um que percebe falhas e um de alerta que avisa alguém sobre inconsistências. Sistemas de monitoramento mais avançados têm um terceiro componente, que corrige alguns dos problemas detectados. Não faz sentido um sistema saber que algo aconteceu, a menos que ele alerte alguém de que há um incidente. Mesmo que o sistema conserte a falha, esse fato deve ser rastreado, pois pode indicar um problema mais profundo, como um bug de software que precisa ser consertado. O objetivo é que o administrador de sistemas perceba as interrupções antes dos clientes. Isto resulta em uma rápida resolução de incidentes além de construir a reputação da equipe de manter um serviço de alta qualidade.(LIMONCELLI; HOGAN; CHALUP, 2017, p. 672).

3.1.2 Ferramentas Típicas para Monitoramento de Redes

Com o aumento do uso de redes de computadores para troca de informações, a regulação e controle dos dados transferidos nessas redes é necessária para garantir a propriedade intelectual de uma organização. Assim, ferramentas de monitoramento de rede altamente personalizáveis que capturam os dados transmitidos na rede continuam sendo projetadas. Muitas dessas ferramentas analisam os dados coletados e fornecem informações valiosas para o usuário.

Ferramentas de monitoramento de rede realizam suas tarefas checando pacotes da rede e filtrando-os com base nas regras especificadas pelo usuário. As ferramentas que oferecem a facilidade de especificar regras simples para a filtragem de pacotes são chamadas de filtros de pacotes. As ferramentas que fazem os pacotes baseados em regras complexas e realizam análises pós-captura dos dados coletados são denominadas ferramentas de monitoramento de rede.

Sabemos que o monitoramento faz parte do gerenciamento de uma rede. E um protocolo bastante utilizado pelas ferramentas de monitoramento é SNMP (Simple Network Management Protocol). O SNMP atua na camada de Aplicação do Modelo OSI e é protocolo padrão para coleta e organização de dispositivos gerenciáveis em redes IP. De acordo com a RFC 3411 o SNMP trabalha com entidades sendo estas apenas simples executoras de comando em rede ou aplicações de monitoramento de

elementos gerenciáveis. Estes elementos podem ser hosts, roteadores, servidores ou qualquer outro dispositivo capaz de se comunicar em uma rede de computadores.

Existem muitas ferramentas de monitoramento de rede disponíveis comercialmente e gratuitamente. Ethereal é uma ferramenta de monitoramento de rede que permite ao operador examinar dados de uma rede em tempo real ou de um arquivo salvo em disco. O operador pode navegar pelos dados capturados, ver o resumo e informações detalhadas para cada pacote e o fluxo de sessões reconstruídas. O Iris é um analisador de tráfego de rede que reporta estatísticas sobre e os componentes destinados à reconstrução da sessão (CAPOOR, 2002).

Atualmente a ferramenta Wireshark é o maior e mais utilizado analisador de protocolos de rede do mundo. Ele permite que você veja o que está acontecendo na sua rede a um nível microscópico e é o padrão de fato em muitas empresas comerciais e sem fins lucrativos, agências governamentais e instituições educacionais. O desenvolvimento da Wireshark prospera graças às contribuições voluntárias de especialistas em rede em todo o mundo e é a continuação de um projeto iniciado por Gerald Combs em 1998. Combs (2019) afirma “(...) nosso objetivo principal é ajudar o maior número possível de pessoas a entender suas redes. Temos sido muito afortunados ao longo dos anos neste sentido. Muitas pessoas são apaixonadas por este objetivo e se dedicaram a ajudar neste trabalho para alcançá-lo” (tradução nossa).

Além das ferramentas citadas acima, o administrador de rede pode-se fazer do uso das aplicações de rede nativas em um sistema operacional. Essas aplicações são geralmente executadas via prompt de comando (Windows) ou a partir de um terminal (distribuições Linux). Confira abaixo algumas delas:

NetStat: Se você estiver tendo problemas com as comunicações em rede, então as estatísticas da rede podem, às vezes, ajudar a apontar para a causa raiz do problema. É aí que entra o comando NetStat. Este comando tem uma série de funções diferentes, mas a mais útil delas é exibir informações resumidas da rede para o administrador. Para ver este tipo de informação resumida, basta digitar NetStat -e.

ARP: O comando ARP corresponde ao Protocolo de Resolução de Endereços. Embora seja fácil pensar em comunicações de rede em termos de endereçamento IP, a entrega de pacotes depende em última instância do endereço MAC (Media Access

Control) do adaptador de rede do dispositivo. Sua função é mapear endereços IP para endereços MAC.

NbtStat: Aos computadores que estão rodando um sistema operacional Windows é atribuído um nome de computador. Muitas vezes, há um nome de domínio ou um nome de grupo de trabalho que também é atribuído ao computador. O nome do computador é às vezes referido como nome NetBIOS. NetBIOS sobre TCP/IP pode ocasionalmente sofrer falhas. O comando NbtStat pode ajudar o administrador a diagnosticar e corrigir tais problemas. O comando NbtStat -n, por exemplo, mostra os nomes NetBIOS que estão em uso por um dispositivo. O comando NbtStat -r mostra quantos nomes NetBIOS o dispositivo tem sido capaz de resolver recentemente.

Tracert: Funcionalmente, o Tracert opera de forma semelhante ao Ping. A maior diferença é que o Tracert envia uma série de requisições ICMP. Isto permite que o utilitário exiba os roteadores pelos quais os pacotes estão passando para serem identificados. Quando possível, o Windows exibe a duração e o endereço IP ou o nome de domínio de cada salto.

NSLookup: é um ótimo instrumento para diagnosticar problemas de resolução de nomes DNS. Basta digitar o comando NSLookup, e o Windows exibirá o nome e o endereço IP do servidor DNS padrão do dispositivo. A partir daí, você pode digitar nomes de host em um esforço para ver se o servidor DNS é capaz de resolver o nome de host especificado.

Route: As redes IP utilizam tabelas de roteamento para direcionar os pacotes de uma sub-rede para outra. O utilitário Route do Windows permite a visualização das tabelas de roteamento do dispositivo. Para fazer isso, basta digitar Route Print. O comando Route não mostra apenas a tabela de roteamento, ele permite que você faça mudanças. Comandos como Route Add, Route Delete e Route Change permitem que você faça modificações na tabela de roteamento, conforme necessário.

Tabela 1 - Lista de Ferramentas para Monitoramento

NOME	LICENÇA	CAMADA (OSI)
Iris	Proprietária	Enlace e Física
Wireshark	Livre	Enlace e Física
NetStat	Livre	Enlace e Rede
NbtStat	Livre	Sessão
ARP	Livre	Enlace e Rede
Tracert	Livre	Rede
NSLookup	Livre	Aplicação
Route	Livre	Rede

Fonte: Elaborado pelo autor (2020)

Como vimos, o monitoramento é fundamental para administração de sistemas. E no que diz respeito a rede de computadores esse método é ainda mais importante. Existem diversas ferramentas de monitoramento utilizadas para as mais diversas situações, entretanto não se deve usar várias ao mesmo tempo pois isso pode comprometer a rede drasticamente.

4 APLICAÇÕES IDEAIS PARA GERENCIAR REDES DE PEQUENO PORTE

Os computadores em rede são capazes de realizar tarefas que nenhum computador poderia realizar. Além disso, as redes permitem que os sistemas de computadores pessoais de baixo custo se conectem a sistemas maiores para executar tarefas que tais sistemas de pequeno e médio desempenho não poderiam executar sozinhos. A maioria das companhias hoje têm uma ou mais redes de computadores. A topologia e o tamanho das redes podem variar de acordo com os sistemas de computador em rede e com o projeto do administrador do sistema. Muitas grandes empresas têm uma mistura sofisticada de redes locais (LANs) e redes de área ampla (WANs) que efetivamente conectam a maioria dos computadores da empresa uns aos outros. A maioria das redes de computadores existentes tem uma arquitetura cliente-servidor, onde uma ou mais máquinas clientes solicitam serviços das máquinas servidoras (tais como sistemas de computadores desktop) (BROWN, HINTERMEISTER, MURPHY, 2007).

As redes de computadores são normalmente geridas por um ou mais "administradores de sistema". Um administrador de sistema é responsável por garantir que a rede funcione sem problemas. Isto significa que este profissional normalmente é responsável por muitas tarefas, incluindo: fazer atualizações de hardware, instalar novo software em servidores, instalar software em máquinas clientes, definir parâmetros de segurança para os recursos da rede, etc. Mesmo em uma rede de pequeno porte se faz necessário, além do administrador de sistema, uma ou mais aplicações para tornar o gerenciamento de dispositivos e usuários mais eficiente e com isso melhorar a produtividade do ambiente de trabalho, seja em um órgão público ou em uma empresa privada (BROWN, HINTERMEISTER, MURPHY, 2007).

Uma complicação para os administradores de sistemas é que muitas redes modernas incluem sistemas de computador que executam diferentes sistemas operacionais, comumente referidos como "plataformas". Cada plataforma tem o seu próprio sistema operativo único. Como resultado, as ferramentas para configurar um sistema de computador cliente são específicas de cada plataforma. Felizmente hoje em dia existem diversas aplicações que trabalham com diferentes plataformas. (BROWN, HINTERMEISTER, MURPHY, 2007).

Constatado a importância do gerenciamento e monitoramento das rede de computadores, principalmente neste mundo cada vez mais virtual, as MPE sofrem um

grande desvantagem nesse aspecto, pois possuem um capital pequeno e pouca base de conhecimento desse ativo, levando a uma competição desleal com as grandes empresas.

Para suavizar esse problema as MPE devem investir em aplicações voltadas para gerenciamento de redes, devendo estas serem balizadas pelos seguintes critérios:

- **Open-source**: pois não possuem custos com pagamento de licenças de uso e manutenção, além de permitir uma maior personalização;
- **Multiplataforma**: devido a heterogeneidade das redes, principalmente com o advento da Internet das Coisas;
- **Transparente**: sendo de fácil instalação e de uso intuitivo sem ser necessário alta especialização;
- **Automação**: permitindo a programação de ações automáticas;
- **Suporte**: para esclarecer dúvidas e buscar soluções para problemas;
- **Atualizado**: fornecendo melhorias que atendam às constantes evoluções tecnológicas.

Com base nesses critérios as MPEs podem escolher aplicações que atenderam às suas necessidades sem gerarem um grande custo operacional.Dito isso selecionamos, logo abaixo, três aplicações de monitoramento de rede que foram analisadas à luz desses critérios:

- **ADVANCED IP SCANNER** - scanner de rede gratuito e confiável para análise LAN. O programa escaneia todos os dispositivos de rede, lhe dá acesso a pastas compartilhadas e servidores FTP, fornece controle remoto dos computadores (via RDP e Radmin), e pode até mesmo desligá-los remotamente. É fácil de usar e é executado como uma edição portátil, ou seja, não precisa instalá-lo na máquina servidora;
- **CACTI** - Cacti é um frontend completo do RRDTool (ferramenta gráfica), ele armazena todas as informações necessárias para criar gráficos e preenchê-los com dados em um banco de dados MySQL. O front-end é completamente guiado por PHP. Além de ser capaz de manter gráficos, fontes de dados e arquivos em um banco de dados, o CACTI também trata da coleta de dados. Há também suporte ao SNMP.

- **ZABBIX** - é um software open-source para monitoramento de redes e aplicações, além disso, a empresa por trás de seu desenvolvimento oferece uma ampla gama de serviços profissionais projetados para atender às demandas comerciais exclusivas de cada cliente. Utiliza templates para as mais diversas situações que uma rede possui.

Existem outras aplicações de monitoramento que não foram analisadas, mas as exemplificaremos aqui para fins de consulta:

- **NAGIOS CORE** - Nagios Core, anteriormente conhecido como Nagios, é um software gratuito e de código aberto que monitora sistemas, redes e infra-estrutura. A Nagios oferece serviços de monitoramento e alerta para servidores, switches, aplicações e serviços.
- **OpenNMS** - OpenNMS é a primeira plataforma de gerenciamento de serviços de rede de código aberto do mundo, e centenas de empresas estão usando-a todos os dias. E, como verdadeiro código aberto, é 100% gratuito.
- **Icinga** - Em toda a sua infra-estrutura, o Icinga lhe dá o poder de observar qualquer host e aplicação. Seu motor de desempenho é capaz de monitorar data centers e sistemas de computação em nuvem. Os resultados coletados são processados e armazenados de uma maneira eficiente em termos de recursos.

Tabela 2 - Lista de Aplicações para Gerenciamento

NOME	CARACTERÍSTICAS	WEBSITE OFICIAL
Advanced IP Scanner	shareware, portátil	advanced-ip-scanner.com
CACTI	intuitivo, gráficos detalhados	cacti.net
Icinga	open-source, vasta comunidade	icinga.com
Nagios	open-source, multiplataforma	nagios.org
OpenNMS	escalonável, extensível, open-source	opennms.com
ZABBIX	open-source, vasta comunidade, multiplataforma	zabbix.com

Fonte: Elaborado pelo autor (2020)

4.1 Análise das Aplicações

Como um dos objetivos específicos propostos nesta pesquisa, devemos apontar a aplicação de monitoramento de rede que melhor atende as necessidades de uma MPE, obedecendo aos critérios antes elencados.

Primeiramente analisaremos o CACTI. É um software livre,o que não geraria custos a uma empresa, porém deve ser usado em conjunto com outra ferramenta (RRDtool) para um melhor aproveitamento. Embora seja uma ferramenta de monitoramento, ela tem foco em geração de gráficos o que é muito utilizado por indústrias e redes de pesquisas. Sendo assim, a rede de computadores de uma MPE não teria a performance desejável ao se utilizar uma aplicação desse porte.

O software Advanced IP Scanner possui várias funcionalidades ideais ao trabalho de um administrador de rede, porém apesar de atender a três critérios, sendo estes a de ser multiplataforma, ter um suporte através de uma empresa e da comunidade online e a de ser transparente, não é open-source o que inibe a adequação da ferramenta de acordo com o ambiente em que for utilizada com a adição de não ser possível a automação de sua aplicação.

O Zabbix cumpre plenamente cinco dos seis critérios apresentados. Apenas pode ser um pouco difícil para o administrador da rede fazer a instalação e

implementação, mas nada que demande uma expertise ou especialização do profissional. O Zabbix é capaz de atender tanto MPE quanto grandes corporações.

Baseando-se na análise das aplicações, constatamos que o ZABBIX é a aplicação que mais atende às carências apresentadas pelas MPE que possuem redes de pequeno porte, devido ao seu leque de ferramentas que proporciona um gerenciamento e monitoramento da rede de forma ativa e autônoma sem ser preciso um alta especialização ou alto custo financeiro.

4.2 ZABBIX

Horst, Pires e Déo (2015, p. 19) em seu livro de A a Zabbix, afirmam que o Zabbix é uma ferramenta moderna, Open Source e multiplataforma, livre de custos de licenciamento, pois sua licença é a General Public Licence versão 2 (GPL). Tem apenas uma versão, que é considerada de classe Enterprise, sendo utilizada para monitorar a disponibilidade e o desempenho de aplicações, ativos e serviços de rede por todo mundo.

Todos os relatórios e estatísticas do Zabbix, assim como os parâmetros de configuração, são acessados através de um front-end. Um front-end baseado na web garante que o estado da sua rede e a saúde dos seus servidores possam ser avaliados a partir de qualquer local. Corretamente configurado, o Zabbix pode desempenhar um papel importante no monitoramento da infra-estrutura de TI. Isto vale tanto para pequenas organizações com poucos servidores como para grandes empresas com uma multiplicidade de servidores.

5 ESTUDO DE CASO: SUPERINTENDÊNCIA DA POLÍCIA RODOVIÁRIA FEDERAL NO ESTADO DO AMAPÁ

5.1 Superintendência da Polícia Rodoviária Federal no Estado do Amapá

A instituição Polícia Rodoviária Federal é um dos órgãos públicos mais importantes do Brasil, cuja as atividades incluem fiscalização das estradas federais, aplicação de multas para infrações cometidas por motoristas, executar operações de busca e apreensão de contrabandos nas rodovias federais dentre tantas outras atividades de vital importância para o Estado e a sociedade.

Figura 1 - Superintendência da Polícia Rodoviária Federal

Fonte:https://selesnafes.com/2018/07/prf-comemora-90-anos-com-previsao-de-novas-unidades-no-ap/

A PRF possui uma superestrutura que conta com, segundo o site da PRF:

> Uma unidade administrativa central, a Sede Nacional, situada em Brasília, e Unidades Administrativas Regionais, representadas por 27 Superintendências (GO, MT, MS, MG, RJ, SP, ES, PR, SC, RS, BA, PE, AL, PB, RN, CE, PI, MA, PA, SE, RO/AC, DF, TO, AM, AP e RR). Além disso, é formada por 150 Subunidades Administrativas e 413 Unidades Operacionais (UOPs), totalizando, assim, mais de 550 pontos de atendimento em todo o Brasil (PRF, [200-?], online).

Toda essa abrangência nacional nos revela a importância desse órgão no Brasil e a sua presença em todos os estados da federação. A PRF tem como missão “Garantir segurança com cidadania nas rodovias federais e nas áreas de interesse da União” (PRF, [2000-?], online), dedicando um esforço tremendo na preservação da ordem pública nas rodovias federais de todos os estados brasileiros.

Todo este empenho no serviço prestado a sociedade, vem da visão de ser reconhecida com um órgão de eficiência e excelência no trabalho policial pela indução de políticas públicas voltadas para a segurança e cidadania.

O estudo de caso foi realizado na Superintendência da Polícia Rodoviária Federal no Estado do Amapá, localizada na Rua Tancredo Neves, 201 no bairro São Lázaro na cidade de Macapá - AP com o CEP 68908-900 (FIGURA 1).

No órgão são prestados serviços essenciais para a sociedade amapaense dentre as quais policiamento ostensivo das rodovias federais e áreas de interesse da União, atendimento ao público, atividade contínua de educação no trânsito, ações sociais na comunidade local (projeto FETRAN), cadastramento de documentos de trânsito nos sistemas online da PRF (SEI, BAT)

A PRF-AP ofereceu um local de trabalho excelente para desenvolvimento das atividades e para aplicação do estudo de caso seguindo a metodologia estabelecida no TCC para a correta obtenção de dados que embasaram a conclusão da pesquisa.

Antes de adentrar-se na parte prática do trabalho, deve-se primeiro conhecer a estrutura da rede de computadores presentes na SPRF-AP para que assim possa ser criado um laboratório de testes que replique o parque tecnológico da sede.

5.2 Infraestrutura e Recursos Humanos

O prédio da SRPRF-AP possui uma estrutura confortável para os trabalhos que são realizados nele, garantindo aos seus funcionários um ambiente climatizado e de livre circulação de ar, tendo um sistema elétrico que respeita as normas da ABNT vigentes no Brasil.

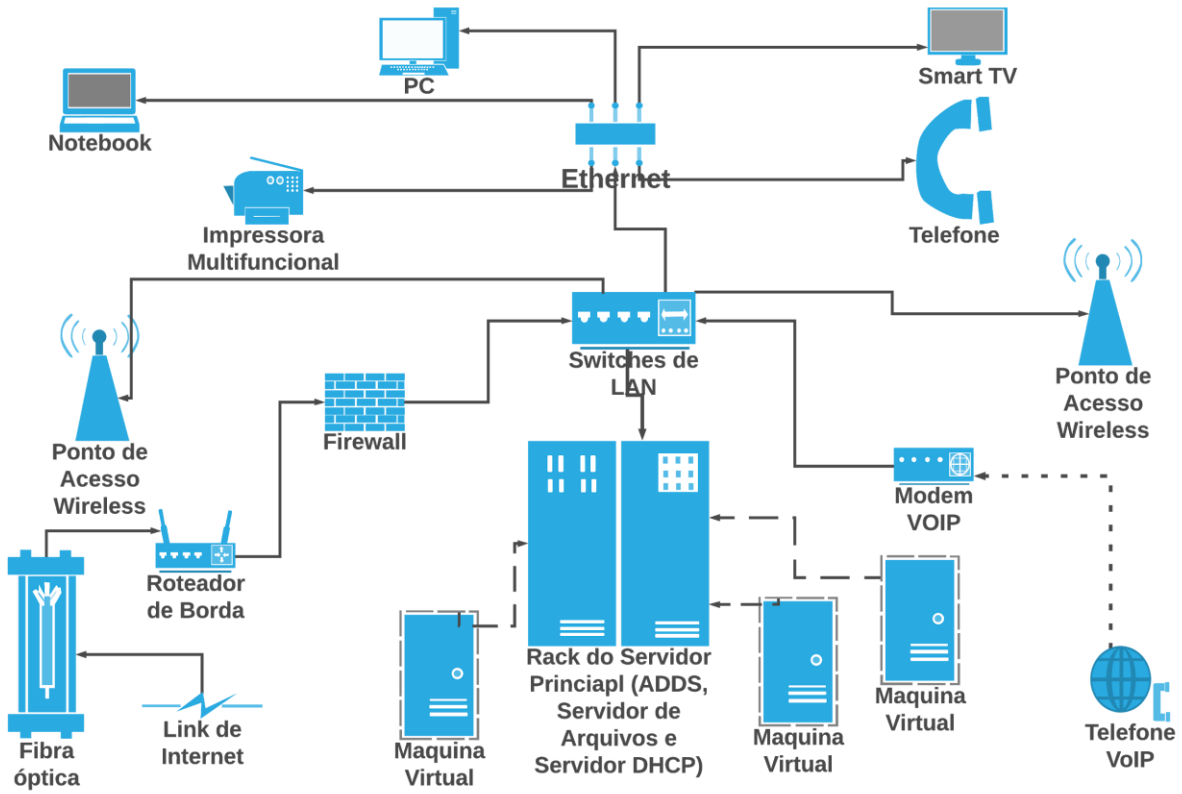
Possui dois links de internet de 20Mb/s e 100Mb/s duplex de velocidade, upload e download com conexão de fibra óptica, além de um cabeamento estruturado implantado seguindo as normas ABNT NBR 14565 com o padrão de conectorização TIA/EIA-568A.

Os principais equipamentos utilizados no órgão são os notebooks, das marcas Positivo e DELL, com sistemas operacionais Windows 7 e 10 PRO, Impressora

multifuncional laser Samsung ProXpress série SLM4070, Servidor Xen com Windows Server 2012 R2 Standard, Roteador da Ruckus e os telefone IP intermediário da INTELBRAS TIP.

O órgão tem implantando na sua rede os serviços do Active Directory, sendo os principais um servidor de arquivos, gerenciamento de contas de usuários e computadores, DHCP, DNS, Firewall de rede e suporte a VPNs (FIGURA 2).

Figura 2 - Estrutura Lógica da Rede SRPRF-AP



Fonte: Elaborado pelo autor (2020)

5.3 Laboratório de Redes para Teste

Dentre as boas práticas na área de redes de computadores é importante que sempre que se for instalar uma nova aplicação na rede deve-se primeiro testá-la em um laboratório de teste para averiguar como a aplicação se comporta no ambiente de produção de forma a prever os possíveis erros de execução e de configuração que poderiam travar a rede da empresa.

O laboratório de teste deve ser feito de forma a replicar a estrutura lógica da rede na qual a aplicação será instalada sem a necessidade de representar a estrutura física.

Para montar o laboratório de redes foram utilizados peças e equipamentos sobressalentes que se encontravam em desuso na sede da PRF como servidores, switches, cabos de rede, patch panel, e um rack do servidor. Veremos suas especificações técnicas no próximo subcapítulo bem como a montagem do mesmo.

5.3.1 Especificações Técnicas

Nesta seção serão elucidadas as especificações técnicas dos equipamentos utilizados no laboratório de rede para testes da aplicação de gerenciamento e monitoramento de redes.

Tabela 3 – Inventário de equipamentos

INVENTÁRIO		
IDENTIFICAÇÃO	**DESCRIÇÃO**	**QUANTIDADE**
Servidor IBM X3400 7976	Processador Intel 8 Core Xeon E3320 1.86 GHz, 4GB de memória RAM, HD de 500 GB.	1
PC Positivo	Intel(R) Pentium(R) CPU G6950 2.80GHz 2 CPUs, 500 GB de HD	1
Server Switch de rack Planet KVM-800	8 portas para conexão VGA e PS/2	1
Switch Intelbras 2400 QR	24 portas Gigabit Ethernet 10/100/1000 Mbps,	1
Patch Panel Cablix CAT5	T568A & T568B	1
VOIP AudioCodes MP-252	Modem ADSL2, Aparelhos DECT, VoIP HD, 802.11 b / g sem fio	1
Cabo Vexans Essential	Cat 6	1
Rack 40 U	Cor Preta	1

Fonte: Elaborado pelo autor (2020)

5.3.2 Instalação e Montagem do Laboratório de Redes

Primeiramente foi necessário fazer uma manutenção básica nos equipamentos, pois sua longa falta de uso gerou-lhes o acúmulo de poeira e a queima de alguns componentes, como placa de rede e disco rígido.

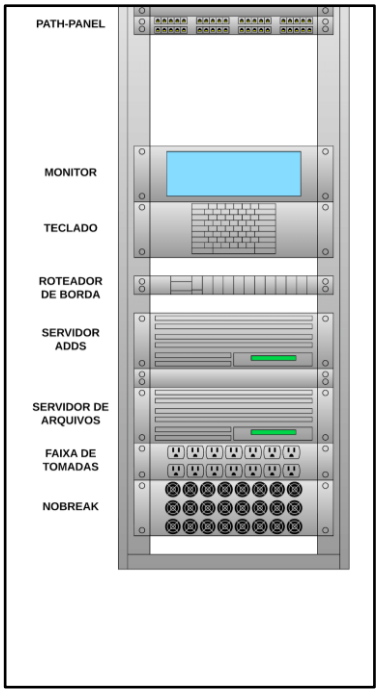
Após a manutenção e o conserto dos equipamentos passamos a montar o rack do servidor de acordo com a planta lógica previamente montada (Figura 3).

Na parte inferior do rack foram colocados o servidor da IBM e o computador de mesa da Positivo na parte frontal e as faixas de tomadas e o nobreak na parte traseira. Logo acima foi instalada a controladora do VOIP.

No centro do rack foi instalado o controlador KVM para teclado, mouse e monitor, conectando-o ao servidor da IBM e da Positivo na parte de baixo.

No topo do rack foram colocados, debaixo para cima, o patch painel e o switch de 24 portas (Figura 4).

Figura 3 - Esquema de Rack do Laboratório de Rede SRPRF-AP



Fonte: Elaborado pelo autor (2020)

No Positivo foi instalado o pfsense 6.4 para atuar como firewall de borda da rede, pois é ele que ficou responsável por proteger o ambiente interno da rede de invasões advindas da internet. A Partir do pfsense a conexão será distribuída para as demais servidores e portas de rede.

O IBM 34088 já vem com a técnica RAID 5 e com o VMware configurada, por isso nele foram criadas 2 máquinas virtuais que foram usadas para instalar o Windows Server 2008 R2 e o Debian para instalação do ZABBIX.

Os detalhes das configurações de cada servidor não são relevantes a pesquisa, por isso concluímos aqui a montagem do laboratório de redes (FIGURA 4)

Figura 4 -Rack do Laboratório de Rede SRPRF-AP

Fonte: Elaborado pelo autor (2020)

5.4 Instalação e Implantação do Zabbix

Segundo Horst, Pires e Déo (p. 26) a instalação do Zabbix pode ser feita por meio de pacotes ou a partir da compilação dos arquivos-fonte. Neste trabalho, optamos por utilizar a forma exemplificada pelo website oficial utilizando uma máquina virtual com Debian 9 (Stretch) e o Zabbix 4.4. A rede foi configurada com a placa da máquina virtual em modo Bridge com permissão de receber todo tráfego da rede local.

Podemos resumir a instalação mínima do Zabbix em três módulos: banco de dados, servidor Zabbix e interface com o usuário (*front-end web*). A seguir será demonstrado o passo a passo da instalação. Os comandos foram executados com privilégio de administrador.

1- Adquirindo privilégios de administrador

```
usuario@usuario:~$ su
senha: (senha de root)
root@usuario:#
```

2 - Instalação do repositório do Zabbix.

Figura 5 – Comandos de instalação do repositório do Zabbix.

```
# wget https://repo.zabbix.com/zabbix/4.4/debian/pool/main/z/zabbix-release/zabbix-release_4.4-1+stretch_all.deb
# dpkg -i zabbix-release_4.4-1+stretch_all.deb
# apt update
```

Fonte: Elaborado pelo autor (2020)

3 - Instalação do servidor Zabbix, *front-end* e agente.

Figura 6 – Comandos de instalação do front-end e agente do Zabbix

```
# apt install zabbix-server-mysql zabbix-frontend-php zabbix-apache-conf zabbix-agent
```

Fonte: Elaborado pelo autor (2020)

4 - Nesta etapa é descrita a instalação do banco de dados. Optamos por utilizar o MySql.

Figura 7 – Comandos de instalação do banco de dados

```
# mysql -uroot -p
password
mysql> create database zabbix character set utf8 collate utf8_bin;
mysql> grant all privileges on zabbix.* to zabbix@localhost identified by 'password';
mysql> quit;
```

Fonte: Elaborado pelo autor (2020)

Depois, foi importado o arquivo de banco de dados para a pasta de instalação do Zabbix. Ao executar o comando foi necessário inserir a senha do banco de dados criada na etapa anterior.

Figura 8 – Comando de importação de arquivos

```
# zcat /usr/share/doc/zabbix-server-mysql*/create.sql.gz | mysql -uzabbix -p zabbix
```

Fonte: Elaborado pelo autor (2020)

5 - Depois foi configurado o banco de dados para o servidor Zabbix. Foi utilizado o editor de textos VIM para modificação do arquivo */etc/zabbix/zabbix_server.conf.*

Figura 9 – Parâmetro configurado no arquivo zabbix_server.conf

```
DBPassword=password
```

Fonte: Elaborado pelo autor (2020)

6 - Após a etapa anterior foi configurado o PHP para o front-end do Zabbix. Aqui também foi utilizado o editor de textos VIM para modificação do */etc/zabbix/apache.conf*. Foi colocado a timezone adequada para a região do Brasil.

 # php_value date.timezone America/Sao_Paulo

7 - Neste penúltimo passo foi iniciado os processos do servidor Zabbix e do agente, e configurados para que iniciem no boot do sistema operacional.

Figura 10 – Comandos de inicialização do Zabbix

```
# systemctl restart zabbix-server zabbix-agent apache2
# systemctl enable zabbix-server zabbix-agent apache2
```

Fonte: Elaborado pelo autor (2020)

8 - Por fim houve a configuração do front-end do servidor Zabbix. Utilizamos o navegador Google Chrome da máquina hospedeira e digitamos na barra de endereços o IP correspondente a máquina onde está instalada o servidor.

http://server_ip_or_name/zabbix

Após configurado bastou acessá-lo com o seguinte login:

- Username: Administrador
- Password: zabbix

5.4.1 Monitoramento da Rede com Templates

Segundo Horst, Pires e Déo (p. 87) um dos recursos que dá mais agilidade ao Zabbix é recurso de *template*. Várias ferramentas suportam esta funcionalidade, entretanto o Zabbix é uma das poucas que suporta o recurso em conjunto com herança de propriedades. Horst, Pires e Déo (p. 88) continuam: Basicamente a template serve para facilitar a vida de quem consegue trabalhar de forma organizada.

Neste trabalho foi configurado as seguintes templates de monitoramento:

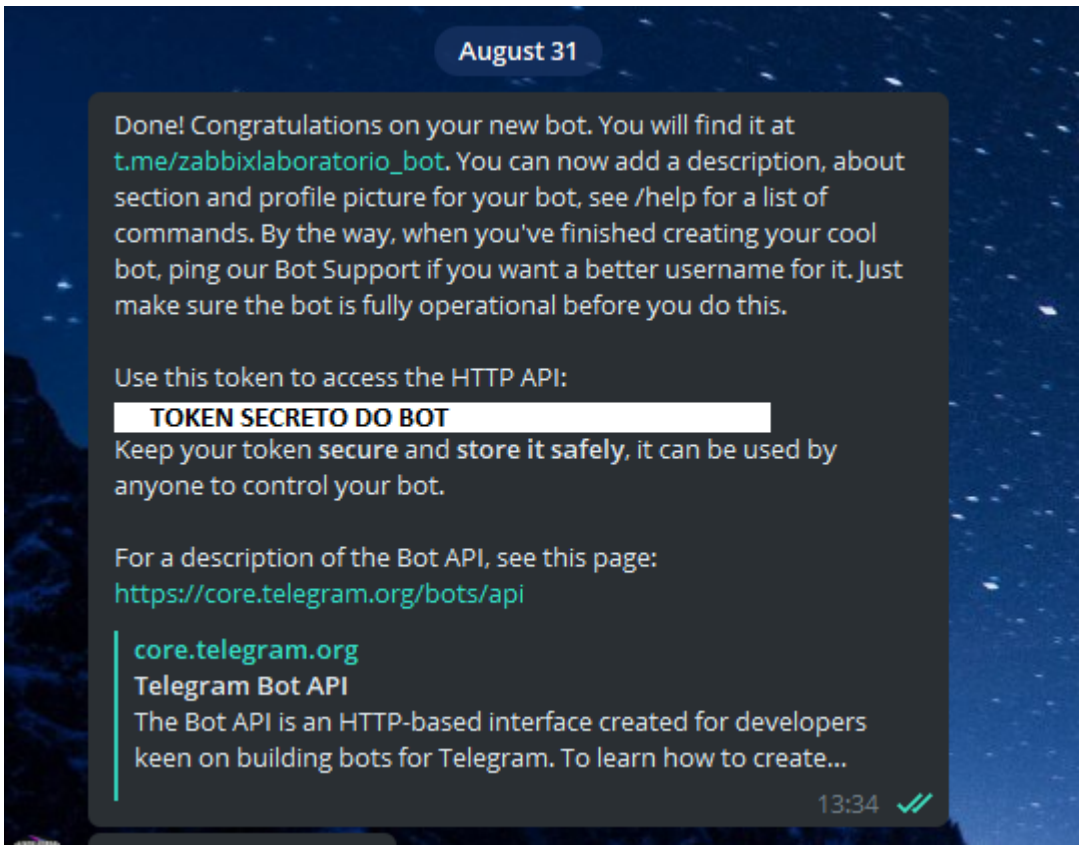
- Verificação de Internet
- Verificação de Host's da LAN

As informações coletadas são salvas no banco de dados do servidor Zabbix. Essas informações só podem ser acessadas pelo administrador da rede.

O Zabbix possui várias formas de enviar alertas ao administrador da rede. Nesta instalação optamos por configurar um bot do Telegram para enviar avisos de incidentes na rede monitorada diretamente para o celular do administrador da rede.
A configuração se deu da seguinte forma:

1- No aplicativo Telegram criamos um novo bot através do @BotFather e seguimos as instruções para configuração do novo bot. Demos o nome de *zabbixlaboratorio_bot.*

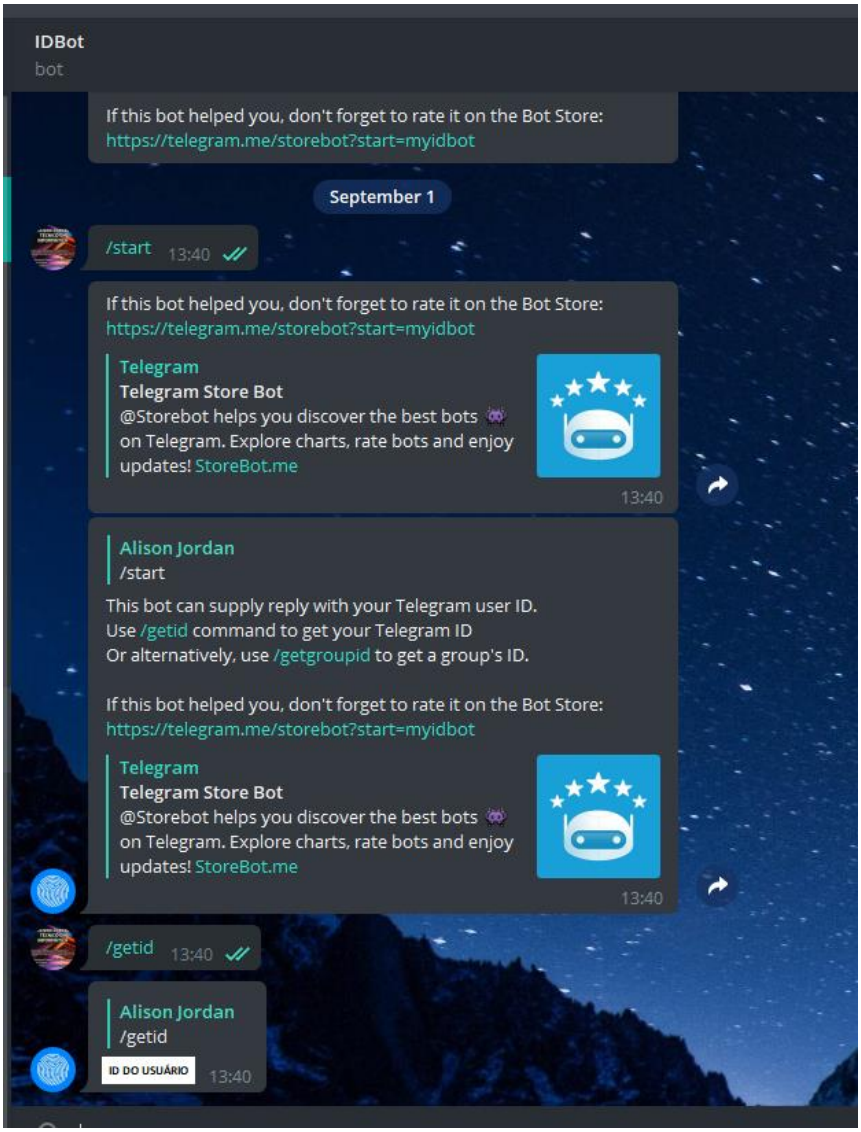
Figura 11 – Criação de Bot no Telegram



Fonte: Elaborado pelo autor (2020)

2- Depois coletamos o ID do usuário do Telegram, o administrador da rede, para que receba as notificações do Zabbix. Para isso utilizamos o IDBot.

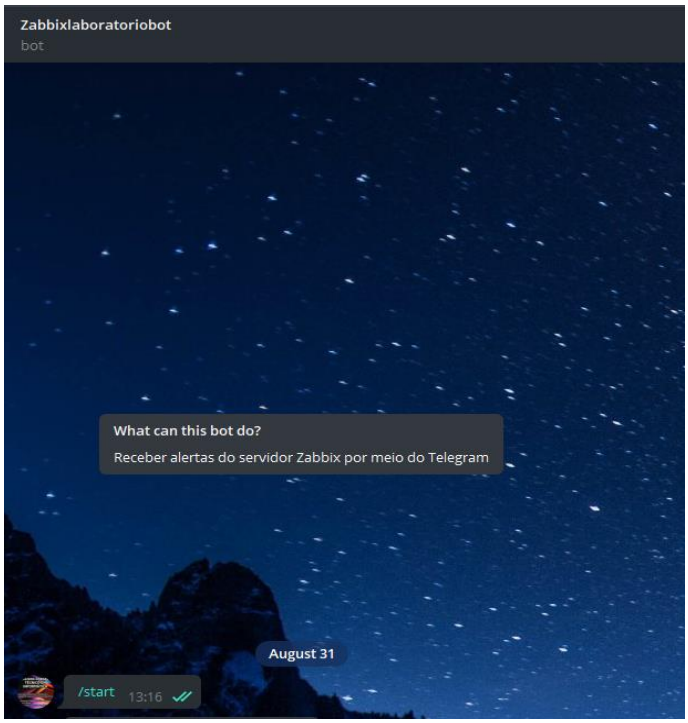
Figura 12 - Captura de ID de usuário no Telegram



Fonte: Elaborado pelo autor (2020)

3- Com o bot criado ainda era necessário iniciá-lo pois não seria capaz de enviar alertas pelo Telegram.

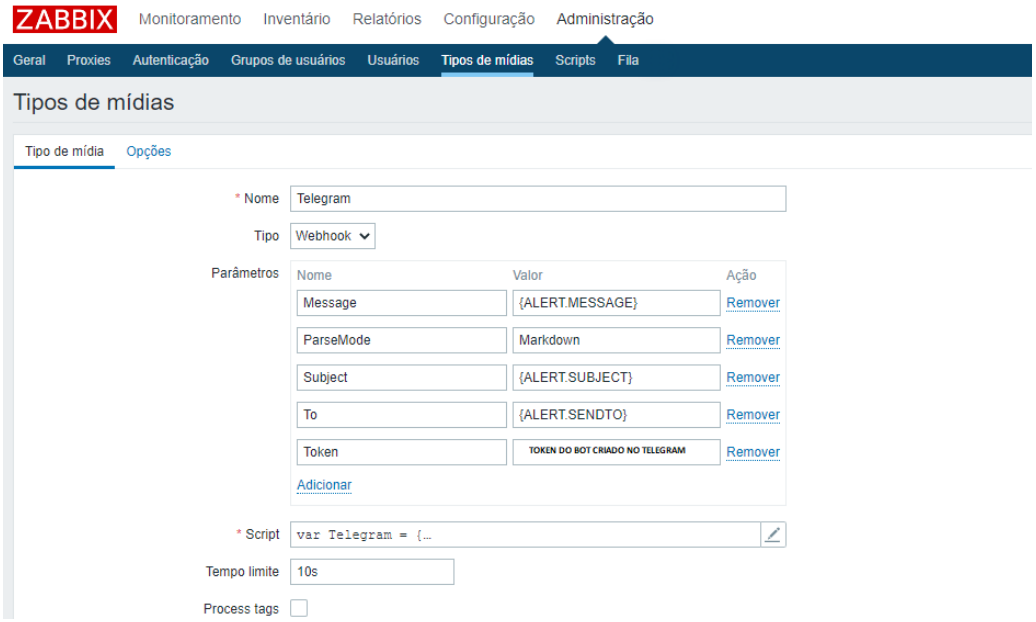
Figura 13 – Inicialização do Bot no Telegram



Fonte: Elaborado pelo autor (2020)

4- No Zabbix bastou configurar o tipo de mídia em Configurações e depois salvar com as informações do bot criado.

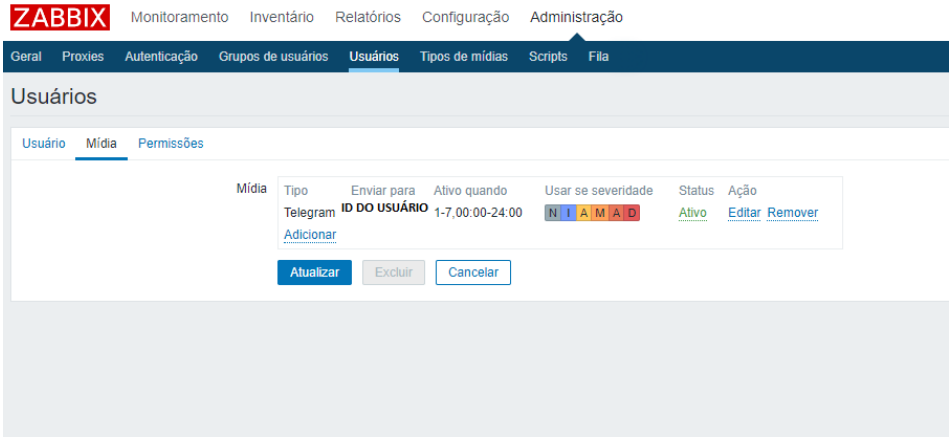
Figura 14 – Configuração do Telegram no Zabbix



Fonte: Elaborado pelo autor (2020)

5- Por fim, foi configurado o usuário Admin do Zabbix com o ID do usuário do Telegram, ou seja, o administrador da rede.

Figura 15 – Vinculação do usuário do Telegram com o usuário Zabbix



Fonte: Elaborado pelo autor (2020)

6 ANÁLISES E RESULTADOS

Primeiramente, para analisarmos os resultados obtidos na pesquisa, devemos relembrar que esse estudo se trata de uma pesquisa básica estratégica com objetivos descritivo e exploratório, que buscou apontar quais são as aplicações voltadas ao gerenciamento de rede ideais a serem adotadas em projeto de redes para MPE no ano de 2020

Adotando o método hipotético dedutivo, levantamos a hipótese de que o ZABBIX é a é a melhor ferramenta de gerenciamento de redes de computadores disponível atualmente no mercado.

Para provar tal hipótese, realizamos um exame bibliográfico, visando identificar quais são os critérios chaves que devemos utilizar na avaliação das ferramentas de gerenciamento de rede, investigando os conceitos gerais que envolvem o tema, como a administração de redes, aliada a governança de TI e seus diferentes modelos, bem como o monitoramento de redes, seus tipos e ferramentas típicas usadas nesse serviço.

Com base nesse exame analisamos três ferramentas voltadas ao gerenciamento de redes, verificando se as mesmas atendem aos critérios encontrados na pesquisa bibliográfica, terminando por validar as ferramentas em um ambiente real por meio de um estudo de caso na Superintendência da Polícia Rodoviária Federal no Estado do Amapá no ano de 2020.

No primeiro capítulo descobrimos o quão importante são administradores de redes de computadores para empresas na atualidade, o que nos levou a compreender que as tarefas executadas por esse profissional como gerir as contas dos utilizadores, gerenciar os servidores, gerenciar a rede de computadores, fazer backups, gerenciar os sistemas da empresa, realizar auditorias e manter atualizado a documentação da rede. são de vital importância para sustentação dos negócios cada vez mais informatizados pelo uso da internet.

Descobrimos também que um administrador de rede pode adotar duas posturas de trabalho, sendo uma Pró-Ativa, onde o administrador realiza revisões periódicas do funcionamento da rede, coletando informações constantemente dos equipamentos monitorados, e a outra Reativa, onde o administrador dedica seu tempo a resolver problemas que surgem diariamente no trabalho e que muitas vezes não tem a ver com suas competências.

Passamos a entender que a Governança de TI, com seus diferentes modelos, faz parte de Governança Corporativa, pois estabelece métodos, processos e normas que devem ser seguidos por todos os funcionários da empresa a fim de manter o parque tecnológico que sustenta o nagóia e que a uma grande diferença em cada modelo de governança de TI, onde cada uma busca uma abordagem diferente para o gerenciamento desse ativo.

No segundo capítulo destacamos a importância do gerenciamento e monitoramento de redes fazendo a análise de três aplicações focadas em ambos segmentos. Além disso exemplificamos ferramentas nativas de SO que podem ser usadas em conjunto com tais programas. Percebemos que há uma ampla gama de ferramentas disponíveis de forma gratuita, cada uma com funcionalidades que melhor se adequam a um negócio específico. Ressaltamos que cabe ao analista de redes escolher aquela que cumprirá a melhor performance.

No terceiro capítulo selecionamos seis critérios que usamos para analisar as três ferramentas de gerenciamento de rede, inspecionando cada uma ponto a ponto.

No quarto capítulo, concluída a pesquisa bibliográfica, realizamos um estudo de caso na Superintendência Regional da Polícia Rodoviária Federal no Amapá no ano de 2020, com intuito de provar a hipótese levantada no início da pesquisa.

Na PRF montamos, primeiramente, como uma das boas práticas na área da informática, um laboratório de testes, fazendo uso de peças sobressalentes que se encontravam em desuso no local.

No laboratório replicamos a estrutura lógica da rede da PRF e instalamos a ferramenta de monitoramento selecionada, detalhado o passo a passo dessa instalação a fim de garantir uma possível replicação do experimento.

Como a instalação da ferramenta não apresentou nenhum problema, passamos para a fase de instalação em ambiente de produção real, porém alguns imprevistos surgiram impedindo a conclusão dessa fase.

O primeiro problema que surgiu foi o fechamento da sede da PRF devido a pandemia de Coronavírus, o que impossibilitou qualquer modificação na rede de computadores a fim de preservar a estabilidade dos serviços já disponíveis.

Outro problema foi a expansão repentina da rede, por meio do Projeto de Rádio Digital que passou a integrar as torres de rádio, bem como um túnel MPLS, ao roteador de borda da sede, aumentando os números de equipamentos a serem monitorados.

Por último a recente política de centralização adoptada pela Secretário de Tecnologia de Informação e Comunicação da PRF em Brasília, visa centralizar todos os serviços e sistemas da PRF, incluindo o monitoramento, em nuvem, sendo esses acessados pelas regionais por meio de uma VPN.

Com base no nosso estudo bibliográfico, notamos que os administradores de rede são responsáveis por manter a parte operacional de um negócio e que por isso necessitam de recursos que os auxiliem na solução de demandas.

Aliados a governança corporativa, concluímos que os administradores de rede devem buscar adotar um modelo de governança de TI, que os direcione na aplicação de normas e processos padronizados que contribuirão para o desenvolvimento do negócio de forma sustentável.

Como os administradores de uma rede de pequeno porte devem se abster de adotar uma postura Reativa no trabalho, eles devem buscar ferramentas de gerenciamento e monitoramento de rede para que possam coletar dados que os ajudem a prever os incidentes na rede e a tomar decisões preventivas que impeçam a interrupção dos trabalhos na empresa.

Tomando por base o pouco capital das MPE para investimento, tanto em mão de obra qualificada como em recursos tecnológicos, catalogamos seis critérios que podem balizar a escolha de uma ferramenta para gerenciamento de rede, sendo estes a de ser open-source, ter suporte a multi plataforma, transparente, possibilitar a automação, dar suporte ao cliente e disponibilizar atualizações.

Utilizando esses critérios, fizemos a análise de três ferramentas de monitoramento de rede, o Advanced IP Scanner, CACTI e o ZABBIX, que estão disponíveis na internet, verificando se eles podem servir como uma ferramenta ideal para as redes de pequeno porte presente nas MPE.

Feita essa análise, constatamos que o ZABBIX é o que melhor atende aos critérios antes identificados, devido ao seu leque de ferramentas que proporciona um gerenciamento e monitoramento da rede de forma ativa e autônoma sem ser preciso um alta especialização ou alto custo financeiro.

Provamos essa conclusão ao instalamos o ZABBIX no laboratório de testes que reproduzia a estrutura lógica da SPRF-AP, pois por mais que tivéssemos poucos recursos e pouca experiência com a ferramenta, conseguimos montar com êxito um sistema de monitoramento de redes.

No início desta pesquisa, tínhamos uma vaga idéia de que o ZABBIX atenderia as necessidades de uma MPE que possui uma rede de pequeno porte, mas agora possuímos a confiança em recomendar o ZABBIX com uma ferramenta a ser utilizada por todas os administradores de rede.

Ao levar em conta a quantidade e complexidade das variáveis que um administrador de redes deve lidar no seu trabalho, seja em uma grande ou pequena empresa, é necessário que se tenha um gerenciamento contínuo de todo os equipamentos tecnológicos da empresa, pois a falha pode acarretar em um desastre financeiro no empreendimento.

Por isso justifica-se o uso do ZABBIX, a medida que o mesmo, apenas com suas ferramentas básicas, nos fornece várias informações da rede em tempo real, controle dos sistemas, notificação de anomalias e automação na resolução de incidentes.

Por fim, levando-se em consideração os assuntos, conceitos e análises abordados na pesquisa, concluímos que o problema foi solucionado, ou seja, o ZABBIX é uma aplicação voltadas ao gerenciamento de rede ideal a ser adotada em projeto de redes para MPE no ano de 2020, porém sempre devemos ter em mente que a tecnologia evolui constantemente e que por isso novas análises devem serem feitas futuramente.

7 CONSIDERAÇÕES FINAIS

Quando se iniciou o trabalho de pesquisa constatou-se que as redes de computadores ganharam um papel relevante na criação e manutenção dos negócios no século XXI e que o gerenciamento dessas redes é imprescindível para sustentação das empresas, porém duvidava-se que as Micro e Pequenas Empresas poderiam competir com as Grandes Empresas em relação a esse ativo.

Diante disso a presente pesquisa teve como objetivo geral elencar as melhores aplicações voltadas ao gerenciamento de redes que possam ser adotadas em projetos de redes para Micro e Pequenas Empresas no ano de 2020, à vista disso vê-se que o objetivo geral foi efetivamente atendido, pois demonstrou-se que o ZABBIX fornece um serviço de gerenciamento de rede satisfatório as necessidades de uma MPE.

O objetivo específico inicial era identificar quais são os pontos importantes a serem observados na gerência da rede de uma MPE, tal objetivo foi atendido por meio da investigação do papel que o administrador de rede desempenha em uma empresa, a importância da Governança de TI para manutenção do parque tecnológico, os tipos de monitoramento de rede e as ferramentas mais usadas nesse serviço, terminando por identificados seis critérios que uma ferramenta de gerenciamento de rede ideal para MPE deve possuir.

O segundo objetivo específico tinha por meta catalogar quais aplicações atendem aos requisitos antes identificados que foi atendido por meio da análise do Advanced IP Scanner, CACTI e o ZABBIX, sendo que o ZABBIX foi o único que atendeu aos requisitos satisfatoriamente.

Já o terceiro e quarto objetivos específicos visavam, respectivamente, implementar as aplicações selecionadas em um ambiente real de produção e por fim avaliar os resultados obtidos na implementação, sendo que o primeiro foi parcialmente atendido, pois foi-se capaz de instalar a aplicação em um laboratório de testes, porém não em um ambiente real, impossibilitando assim a resolução do quarto objetivo específico.

Partiu-se da hipótese de que o Zabbix é a melhor ferramenta de gerenciamento de redes de computadores disponível atualmente no mercado pois, além de ser open-source, companhias ao redor do mundo de forma a demonstrar grande confiança nas suas soluções e avançada performance.

Durante a execução da pesquisa descobriu-se que as MPE podem balizar a escolha de uma ferramenta de gerenciamento de rede em seis critérios e que o ZABBIX é o único que atendia a cinco desses critérios dentre as ferramentas analisadas, terminando por confirmar a hipótese levantada no início da pesquisa.

Portanto conclui-se que o problema que originou a pesquisa foi solucionado satisfatoriamente, uma vez que se identificou o ZABBIX como uma aplicação voltada ao gerenciamento de rede ideal a ser adotada em projeto de redes para MPE no ano de 2020.

A presente pesquisa buscou solucionar o problema por meio da análise de obras e documentos voltados a administração de redes, governança de TI, gerenciamento e monitoramento de redes, a fim de identificar os pontos essenciais que um gerenciamento de rede deve atender em uma MPE, sendo que tal descoberta possibilitaria fazer a análise das ferramentas previamente selecionadas para pesquisa, tendo por fim validar a ferramenta em um ambiente real.

Diante da metodologia proposta percebe-se que a pesquisa poderia ter se aproveitado das experiências de profissionais da área de rede, por meio de entrevista, com intuito de entender melhor as dificuldades que os mesmos encontram no trabalho.

Poderia ter aumentado o escopo, analisando mais ferramentas e testando-as todas em ambiente real, a fim de coletar dados mais calcados na prática, pois a aplicação em um ambiente de produção, ou seja, na rede de uma pequena empresa foi impedida por diversos fatores.

Sugere-se que seja feita uma pesquisa mais aprofundada no dia a dia dos administradores de rede de Micro e Pequenas Empresa, as dificuldades encontradas no trabalho, a forma como solucionaram os problemas na rede, se põem em prática melhorias na sua atividade, se buscam mais qualificação profissional e se tem apoio da empresa em que trabalham para aplicar melhorias e novas tecnologias.

Sugere-se também a pesquisa de formas de automação na resolução de incidentes na rede e como essa prática afetaria o trabalho dos administradores de redes, bem como o impacto nos negócios informatizados.

REFERÊNCIAS

ABREU, Vladimir Ferraz de; FERNANDES, Aguinaldo Aragon. **Implantando a Governança de TI:** *de estratégia à gestão dos processos e serviços*. 5. ed. Rio de Janeiro: BRASPORT Livros e Multimídia Ltda. 2012.

ALVES, Luiz. Comunicação de Dados. 2. ed. São Paulo: Makron Books. [1992 ou 1994]. p. 287, 288.

BROWN, Kenneth; HINTERMEISTER, Gregory; MURPHY, Michael. **Apparatus and method for managing configuration of computer systems on a computer network**. Google Patents, 2007. Disponivel em: <https://patents.google.com/patent/US7171458B2/en>. Acesso em: 17 fev. 2020.

CAPOOR, Neraaj. **Design and Implementation of a Network Monitoring Tool**. CiteSeer^{X}, 2002. Disponivel em: <http://citeseerx.ist.psu.edu/viewdoc/citations;jsessionid=DD76D6D297C14968A7711F2ACB6F70B7?doi=10.1.1.10.2426>. Acesso em: 17 fev. 2020.

COMBS, Gerald. **Dedication and Disagreements**. Wireshark, 2019. Disponivel em: <https://blog.wireshark.org/2019/07/dedication-and-disagreements/>. Acesso em: 24 fev. 2020.

FILHO, Olavo Poleto. **Gerenciamento e Monitoramento de Redes**: *Análise de Desempenho*. 2012. Disponivel em: <https://www.teleco.com.br/tutoriais/tutorialgmredes1/default.asp>. Acesso em: 13 abr. 2020.

G1. **Empresas buscam serviços gerenciados para focar nos negócios**. Disponivel em: <http://g1.globo.com/economia/especial-publicitario/embratel/pense-inovacao/noticia/2015/01/empresas-buscam-servicos-gerenciados-para-focar-nos-negocios.html>. Acesso em: 10 fev. 2020.

HORST, Adail; PIRES, Aécio; DÉO, André. **De A a Zabbix**. 1. ed. São Paulo: Novatec. 2012. p. 19, 26, 87 e 88.

ISACA. **COBIT 5**:*Modelo Corporativo para Governança e Gestão de TI da Organização*. Disponivel em: <https://www.isaca.org/>. Acesso em: 05 mar. 2020.

LIMONCELLI, Thomas; HOGAN, Christina; CHALUP, Strata. **The Practice of System and Network Administration**. 3. ed. Estados Unidos: Addison-Wesley. 2017. p. 671, 672.

LUCIANO, Ribeiro. **Internet no Brasil**: *Estatísticas e Projeções*. Disponivel em: <https://blog.arriminum.com/internet-no-brasil-estatisticas>. Acesso em: 10 fev. 2020.

NASCIMENTO, Jefferson. **Governança de TI e a ISO/IEC 38500**. Portal GSTI, 2009. Disponivel em: <https://www.portalgsti.com.br/2009/11/governanca-de-ti-e-isoiec-38500.html>. Acesso em: 09 mar. 2020.

SATO, Danilo. **DevOps na Prática:** *entrega de software confiável e automatizada*. 1. ed. São Paulo: Casa do Código. [201-]. p. 06.

SEBRAE. **Pequenos negócios em números**. Disponivel em: <https://www.sebrae.com.br/sites/PortalSebrae/ufs/sp/sebraeaz/pequenos-negocios-em-numeros,12e8794363447510VgnVCM1000004c00210aRCRD>. Acesso em: 10 fev. 2020.

SELESNAFES.COM. **PRF comemora 90 anos com previsão de novas unidades no AP**. Disponível em: <https://selesnafes.com/2018/07/prf-comemora-90-anos-com-previsao-de-novasunidades-no-ap/>. Acesso em: 01 jun. 2019.

SOUSA, Lindeberg Barros de. **Projetos e Implantação de Redes**:*fundamentos, arquiteturas, soluções e planejamento*. 3. ed. São Paulo: Érica. 2013. p. 301, 305.

TELES, Fabio. **O que é governança de TI e qual a sua relevância para as organizações?**. Desk Manager, 2017. Disponivel em: <https://blog.deskmanager.com.br/o-que-e-governanca-de-ti/>. Acesso em: 01 mar. 2020.

VUMO, Ambrósio Patrício.**Administração de Redes de Computadores**. Universidade Virtual Africana, 2017. Disponivel em: <https://oer.avu.org/bitstream/handle/123456789/646/CSI%205300%20Administrac%CC%A7a%CC%83o%20de%20Redes%20de%20Computadores1%20.pdf?sequence=1&isAllowed=y>. Acesso em: 01 mar. 2020.

Zabbix Manual. Disponível em <https://www.zabbix.com/documentation/current/manual>. Acesso em 21 de janeiro de 2020.

Zabbix + Telegram. Zabbix, 2020. Disponivel em: <https://www.zabbix.com/integrations/telegram>. Acesso em: 31 ago. 2020.

ANEXO A – TERMO DE AUTORIZAÇÃO

MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA
POLÍCIA RODOVIÁRIA FEDERAL
SUPERINTENDÊNCIA DA POLÍCIA RODOVIÁRIA FEDERAL NO AMAPÁ

TERMO DE AUTORIZAÇÃO PARA DIVULGAÇÃO DE INFORMAÇÕES DE ORGÃOS PÚBLICOS

Razão Social: SUPERINTENDÊNCIA DA POLÍCIA RODOVIÁRIA FEDERAL NO ESTADO DO AMAPÁ

CNPJ: 00.394.494/0140-05 Inscrição Estadual: Isento

Endereço completo: Rua Tancredo Neves, nº 201, Bairro São Lázaro Macapá - AP, 68908-900

Nome do Responsável: ALDO BALIEIRO MACHADO Função: Superintendente

Telefone: (96) 3225-9000 e-mail: aldo.balieiro@prf.gov.b

Tipo de produção intelectual: ( ) Monografia; (X) TCC; ( ) Relatório de Estágio;
( ) Dissertação; ( ) Tese; ( ) Outro:

Título/subtítulo: ESTUDO DE CASO NA IMPLEMENTAÇÃO DE SERVIÇOS DE GERENCIAMENTO E MONITORAMENTO EM UMA REDE DE PEQUENO PORTE

Autor: ADSON JAIRO DE LIMA ROSA Código de matrícula: 2017210110023

Autor: ALISON JORDAN DE LIMA ROSA Código de matrícula: 2017210110022

Orientador: KLENILMAR LOPES DIAS

Nome do Curso: Curso Superior de Tecnologia em Redes de Computadores

Câmpus: INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO AMAPÁ - CAMPUS MACAPÁ

Como representante da empresa acima nominada, declaro que as informações e/ou documentos disponibilizados pela empresa para o trabalho citado:

[X] Podem ser publicados sem restrição.

( ) Possuem restrição parcial por um período _____ anos, não podendo ser publicadas as seguintes informações e/ou documentos:

( ) Possuem restrição total para publicação por um período de _____ anos, pelos seguintes motivos:

Representante do Orgão

Macapá, 09/12/2020
Local e Data