INSTITUTO FEDERAL DO SUDESTE DE MINAS GERAIS

CÂMPUS AVANÇADO BOM SUCESSO.

TECNOLOGIA EM ANÁLISE E DESENVOLVIMENTO DE SISTEMAS.

ÉRICA SANTOS MARTINS

FERRAMENTAS DE MONITORAMENTO DE REDE: UMA COMPARAÇÃO TEÓRICA ENTRE NAGIOS, CACTI E ZABBIX.

BOM SUCESSO - MG
2024

ÉRICA SANTOS MARTINS

FERRAMENTAS DE MONITORAMENTO DE REDE: UMA COMPARAÇÃO TEÓRICA ENTRE NAGIOS, CACTI E ZABBIX.

Trabalho de Conclusão de Curso apresentado ao Câmpus Avançado Bom Sucesso, do Instituto Federal de Educação Ciência e Tecnologia do Sudeste de Minas Gerais, como parte das exigências do curso de Graduação em "Tecnologia em Análise e Desenvolvimento de Sistemas" para a obtenção do título de Tecnólogo.

Orientador: Prof. Antônio Rafael Sant'Ana.

BOM SUCESSO - MG
2024

Dados internacionais de catalogação na publicação (CIP)
Bibliotecária responsável Maria de Lourdes Cardoso CRB-6/3242

M379f Martins, Erica Santos

Ferramentas de monitoramento de rede : uma comparação teórica *Nagios, Cacti e Zabbix* [recurso eletrônico] / Erica Santos Martins; Bom Sucesso, MG: IFSUDESTEMG, 2024.

38 p. ; 23 cm.

Orientador: Antônio Rafael Sant'anna
Trabalho de Conclusão de Curso (Tecnólogo em Análise e desenvolvimento de sistemas).

1. Tecnologia da informação. 2. Software livre. 3.Internet. I. Sant'anna, Antônio Rafael. II. Instituto Federal do Sudeste de Minas Gerais, Campus São João Del Rei. III. Título.

CDD: 005.1

TERMO DE APROVAÇÃO

ÉRICA SANTOS MARTINS

FERRAMENTAS DE MONITORAMENTO DE REDE: UMA COMPARAÇÃO TEÓRICA ENTRE NAGIOS, CACTI E ZABBIX.

Este Trabalho de Conclusão de Curso foi julgado e aprovado como requisito parcial para a obtenção do grau de Tecnólogo em Análise e Desenvolvimento de Sistemas do Instituto Federal de Educação, Ciência e Tecnologia do Sudeste de Minas Gerais — *Campus* Avançado Bom Sucesso.

Bom Sucesso, 9 de setembro de 2024.

Assinaturas:

gov.br Documento assinado digitalmente
ANTONIO RAFAEL SANT ANA
Data: 15/10/2024 14:05:02-0300
Verifique em https://validar.iti.gov.br

Membro da Banca

gov.br Documento assinado digitalmente
DENISSON NEVES MONTEIRO
Data: 15/10/2024 14:01:31-0300
Verifique em https://validar.iti.gov.br

Membro da Banca 2

gov.br Documento assinado digitalmente
JOSE GELSON GONCALVES
Data: 15/10/2024 12:36:37-0300
Verifique em https://validar.iti.gov.br

Membro da Banca 3

Dedico este trabalho a Deus, pelas forças e sabedoria concedidas ao longo do curso, e a mim, por não desistir e acreditar que, com fé, força e dedicação, podemos alcançar grandes conquistas.

AGRADECIMENTOS

Gostaria de dedicar meu sincero agradecimento a todas as pessoas que foram fundamentais na concretização deste trabalho:

Primeiramente, expresso minha gratidão a Deus, cuja orientação e força foram essenciais para superar os desafios ao longo desta jornada acadêmica.

Aos meus queridos pais, Luciana e Flaviano, agradeço por sua inestimável dedicação na minha criação, educação e por serem o suporte inabalável que sempre esteve ao meu lado, encorajando-me a cada passo deste percurso.

Ao Professor Antônio Rafael Sant'Ana, meu orientador, agradeço por aceitar o desafio de guiar este trabalho.

Aos demais professores, colegas e colaboradores da instituição, meu agradecimento pelo valioso suporte, ensinamentos e contribuições que enriqueceram minha jornada acadêmica, tornando-a mais rica e proveitosa.

“Talvez não tenha conseguido fazer o melhor, mas lutei para que o melhor fosse feito. Não sou o que deveria ser, mas Graças a Deus, não sou o que era antes”.

(Marthin Luther King 1929-1968)

RESUMO

O avanço tecnológico e a pandemia de COVID-19 aceleraram a migração para ambientes digitais, destacando a importância da infraestrutura e do monitoramento de redes. A *internet*, sustentada por *software*, *hardware* e cabos de fibra *óptica*, é fornecida por provedores e operadoras, exigindo o uso de ferramentas eficazes para assegurar a qualidade dos serviços. Este trabalho, que utiliza o método de pesquisa descritiva, tem como objetivo geral analisar e destacar as capacidades dos *softwares* de monitoramento *Zabbix*, *Nagios* e *Cacti*, e observar suas funcionalidades no contexto da garantia da qualidade operacional das redes de telecomunicações e infraestrutura de TI. A análise fundamenta-se em artigos nos quais os autores testaram essas ferramentas como critério principal. Com base na análise realizada neste trabalho e na eficiência da utilização do monitoramento, desenvolve-se uma proposta para a implementação de ferramentas de monitoramento no IF Sudeste MG - Campus Avançados Bom Sucesso, com o objetivo de otimizar a infraestrutura de TI. Portanto, o trabalho destaca as capacidades e a eficiência de cada ferramenta e conclui que a escolha e a implementação dependerão das necessidades do usuário e dos requisitos específicos para sua utilização.

Palavras-chave: ferramentas de monitoramento; avanço tecnológico; *internet.*

ABSTRACT

Technological advancement and the COVID-19 pandemic have accelerated the migration to digital environments, highlighting the importance of infrastructure and network monitoring. The internet, sustained by software, hardware and fiber optic cables, is provided by providers and operators, requiring the use of effective tools to guarantee the quality of services. This work, which uses the descriptive research method, has the general objective of analyzing and highlighting the capabilities of Zabbix, Nagios and Cacti monitoring software, and observing their functionalities in the context of ensuring the operational quality of telecommunications networks and IT infrastructure. The analysis is based on articles in which the authors tested these tools as the main criterion. Based on the analysis carried out in this work and the efficiency of using monitoring, a proposal is developed for the implementation of monitoring tools at IF Sudeste MG - Campus Avançados Bom Sucesso, with the aim of improving the IT infrastructure. Therefore, the work highlights the capabilities and efficiency of each tool and concludes that the choice and implementation depend on the user's needs and the specific requirements for its use.

Keywords: monitoring tools; technological advancement; internet.

SUMÁRIO

1 INTRODUÇÃO

Em virtude do cenário atual, marcado por avanços tecnológicos constantes, observa-se um notável aumento do interesse das pessoas nos recursos disponibilizados pela tecnologia. Esse fenômeno é impulsionado pela facilidade de acesso à *internet*, que já se tornou parte do nosso cotidiano. Os recursos computacionais estão se tornando cada vez mais evidentes, influenciando praticamente todos os aspectos de nossas vidas.

Pode-se dizer que essa revolução digital teve um salto maior com a chegada da pandemia da COVID-19[1] em 2020 onde fomos obrigados a migrar para o ambiente digital. A necessidade de distanciamento social impulsionou a adoção de ferramentas de videoconferência, comércio eletrônico, trabalho home office, estudos em EAD (Ensino à Distância) e outras tecnologias *on-line*. Nesse contexto, Tuma (2022, p. 59) observa que "em um curto espaço de tempo, trabalhadores e empresas tiveram suas vidas transformadas, tendo que se adaptar às possibilidades que o teletrabalho proporcionou." Ou seja, passamos a depender mais da *internet* e isso tem levado os usuários a procurarem cada vez mais por serviços de banda larga ou planos de telefonia 4G/5G.

Sabemos que essa comunicação global se dá devido à *internet*, mas afinal, como ela chega exatamente até nós? Em resumo, pode-se dizer que a *internet* envolve dois elementos essenciais, sendo eles o software e o hardware, que nada mais são que componentes físicos e lógicos responsáveis pela transmissão, recepção e processamento de dados em toda a rede. A *internet* se conecta pelo mundo todo através de cabos de fibra *óptica* que compõem o *backbone*, onde interligam os continentes. É a partir dessa infraestrutura que as operadoras distribuem a conectividade até nossas residências.

A distribuição da *internet* para o usuário final ocorre por meio dos provedores de serviços de *internet* (ISP), que contratam a infraestrutura das operadoras. No entanto, atualmente, as próprias operadoras também estão se encarregando de fornecer diretamente a conectividade aos usuários. Isso ocorre devido ao aumento da demanda por esses serviços, o que está gerando receita e, consequentemente, chamando a atenção das operadoras para uma maior integração vertical em sua cadeia de valor.

---

[1] COVID-19-*Corona Virus Disease* 2019

Neste cenário, devido ao aumento do consumo de dados e a crescente demanda por conectividade, os provedores e operadoras de telecomunicações enfrentam desafios significativos onde, para lidar com essa evolução digital, estão implementando cada vez mais uma série de estratégias, bem como investimentos em infraestrutura de rede de alta capacidade. Outro ponto importante também é manter a qualidade de seus serviços que já são utilizados, isso inclui a importância de se ter um monitoramento da rede.

O monitoramento eficaz das redes de telecomunicações torna-se essencial para identificar e resolver problemas de forma ágil, além de antecipar a resolução antes mesmo que os usuários percebam qualquer falha. Dentre as diversas ferramentas disponíveis no mercado, algumas têm se destacado, tais como *Zabbix, Nagios, Cacti* e *Icinga*, pois oferecem recursos e funcionalidades para acompanhar o desempenho de redes, servidores e aplicativos. Suas capacidades de monitorar em tempo real, alertar sobre eventos críticos e fornecer análises detalhadas tornam-nas uma excelente escolha para provedores de telecomunicações que buscam aprimorar a eficiência operacional e garantir a qualidade de seus serviços

Portanto, considerando esses aspectos, o presente trabalho propõe explorar a implementação e os recursos dos principais *softwares* de monitoramento de rede, com base em artigos e trabalhos acadêmicos onde os autores testaram essas ferramentas. Além disso, serão analisadas as vantagens e desvantagens, os desafios de utilização e as melhores práticas associadas à sua integração na rede, visando fornecer autoconhecimento para profissionais do setor interessados em aprimorar suas estratégias de monitoramento e oferecer percepções valiosas fundamentadas em experiências reais.

1.1 OBJETIVOS

1.1.1 Objetivo geral

Este trabalho tem como objetivo geral analisar e destacar as capacidades dos softwares de monitoramento, bem como observar suas funcionalidades e como são utilizadas para garantir a qualidade operacional das redes de telecomunicações e infraestrutura de TI. Isso inclui a identificação de áreas de melhoria e possíveis soluções para otimizar a eficiência do monitoramento, contribuindo para o avanço do conhecimento na área de identificação de falhas dentro de uma infraestrutura de rede de acesso.

Busca-se também oferecer diretrizes práticas para a implementação eficaz de *softwares* de monitoramento em ambientes semelhantes, com o objetivo de elevar a excelência dos serviços fornecidos não somente por operadoras e provedores de telecomunicações como também outras áreas de interesse.

1.1.2 Objetivos específico

- Identificar os principais desafios enfrentados pelas operadoras e provedores de telecomunicações no contexto da evolução digital;

- Realizar pesquisas a fim de ampliar os conhecimentos relacionados aos *softwares* de monitoramento mais utilizados;

- Observar as funcionalidades e recursos oferecidos.

1.2 JUSTIFICATIVA

Com o crescimento do uso da internet e dos serviços digitais, os provedores de telecomunicações enfrentam desafios crescentes para garantir a qualidade e a disponibilidade de seus serviços. A ausência de um monitoramento eficaz de redes pode resultar em falhas de serviço, lentidão, e interrupções, levando a insatisfação dos usuários e à perda de clientes. Nesse contexto, justifica-se a análise e a ênfase na importância da implementação de ferramentas de monitoramento, como os principais softwares utilizados. Este estudo tem

como objetivo demonstrar e orientar os profissionais da área sobre a eficácia dessas ferramentas para identificar e resolver problemas de rede de forma proativa, minimizando os impactos negativos na experiência do usuário e assegurando a continuidade dos serviços oferecidos.

2 REFERENCIAL TEÓRICO

2.1 EVOLUÇÃO DA *INTERNET* E SEU IMPACTO NA INFRAESTRUTURA DE TELECOMUNICAÇÕES

De acordo com os Kurose e Ross (2013) “A *internet* é uma rede de computadores que interconecta centenas de milhões de dispositivos de computadores ao redor do mundo”. Em um passado próximo não era comum a utilização desta conexão igual aos dias atuais. Quando se mencionava a *internet*, pensávamos apenas em computadores de mesa, com conexões lentas e, ocasionalmente, modems para notebooks, mas ainda sem a rápida acessibilidade que temos nos dispositivos móveis atualmente.

Nos últimos anos, temos vivenciado o domínio mundial da *internet*, um fenômeno que também é conhecido como a “*Internet* das Coisas”, caracterizado pela interconexão de vários produtos. Esta tendência tem possibilitado desde a conexão de dispositivos simples até mesmo a automação completa de residências. É importante compreender que a *internet* vai muito além de apenas uma conexão Wi-Fi ou dados móveis para realização de pesquisa ou a utilização das redes sociais, e por esse motivo é considerado importante saber mais sobre sua estrutura e funcionamento mesmo que seja de forma básica.

A *Internet* das Coisas (IoT) surgiu como uma área de crescente interesse e pesquisa. Os autores Santos *et al*. (2024), aborda que "A *Internet* das Coisas, em poucas palavras, nada mais é que uma extensão da *Internet* atual, que proporciona aos objetos do dia-a-dia (quaisquer que sejam), mas com capacidade computacional e de comunicação, se conectarem à *Internet*”. Essa definição destaca a capacidade dos objetos cotidianos de se tornarem interconectados e inteligentes, transformando a maneira como interagimos com o mundo ao nosso redor.

De acordo com a publicação realizada no sistema de gerenciamento de bancos de dados ORACLE (c2022), atualmente existe um número aproximado de 10 bilhões de aparelhos IOT que estão conectados à *internet*, mas com possibilidade de ter este número dobrado com o decorrer dos anos.

Nesse cenário, os provedores e operadoras de telecomunicações desempenham um papel essencial como facilitadores dessa interconexão. Eles fornecem a infraestrutura

necessária para suportar a crescente demanda por conectividade, garantindo que os dispositivos IoT possam se comunicar de forma eficiente e confiável.

No entanto, os desafios não se limitam apenas à infraestrutura física. Os provedores também precisam lidar com questões de segurança, privacidade e escalabilidade. A proteção dos dados transmitidos entre dispositivos e servidores é fundamental para evitar vulnerabilidades e ataques cibernéticos. Além disso, à medida que mais dispositivos são adicionados à rede, a capacidade de dimensionamento se torna importante para manter a qualidade do serviço, sendo essencial também aderir ao monitoramento contínuo da rede.

2.2 ISP (PROVEDORES DE SERVIÇOS DE *INTERNET*) E SUA INFRAESTRUTURA

Os Provedores de Serviços de *Internet*, conhecido também por sua sigla ISP, têm um papel importante em relação à conectividade mundial, pois é através deles que hoje temos milhares de usuários conectados simultaneamente à rede. A origem dos ISP está relacionada ao crescimento e à expansão da web ao longo das últimas décadas. Inicialmente, a *Internet* era utilizada apenas por instituições acadêmicas e militares, com acesso limitado a um pequeno número de usuários. No entanto, com a chegada da World Wide Web, nossa famosa WWW e também o desenvolvimento de tecnologias de rede, a *Internet* tornou-se acessível ao público em geral.

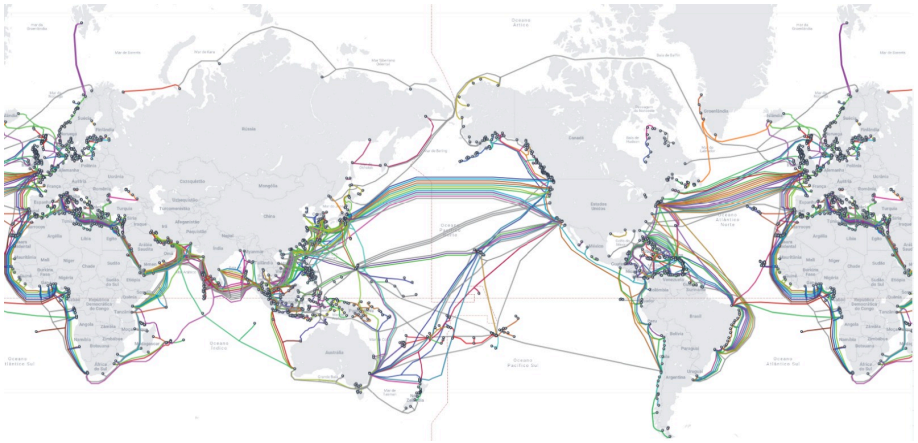
Os autores Paula e Regina (1999) afirmam que "para que um usuário qualquer possa acessar a *Internet* a partir de seu microcomputador, é necessário que ele seja autorizado por um provedor de acesso." Os provedores de *internet* possuem uma interconexão que requer uma infraestrutura capaz de acompanhar os avanços tecnológicos, garantindo assim a qualidade contínua de seus serviços.

Os autores Kurose e Ross (2013) classificam os provedores de acesso à *internet* como de nível alto e baixo, dependendo de sua infraestrutura. De acordo com eles, "Um ISP de nível mais alto consiste em roteadores de alta velocidade interconectados com enlaces de fibra *óptica* de alta velocidade." Por sua vez, "Cada rede ISP, seja de nível mais alto ou mais baixo, é gerenciada de forma independente." Essa autonomia de gestão permite aos provedores adaptar suas operações às necessidades específicas dos usuários e às demandas do mercado,

promovendo assim a diversidade e a inovação no setor de serviços de *internet*, para a evolução contínua da infraestrutura de comunicação global.

Atualmente a infraestrutura mais utilizada pelos ISP são interligadas através de *backbones* intercontinental e interestadual que são compostos por cabos de fibra *óptica*, esses cabos são conectados em pontos de presença conhecidos como PoPs, em que possui equipamentos como *switch* de grande porte e posteriormente roteadores com alta capacidade de direcionamento de rotas. De acordo com o mapa de cabos submarinos disponível em *Submarine Cable Map*, podemos observar a extensa rede de comunicações submarinas.

Figura 1: Mapa de cabos submarinos.



Fonte: Submarine Cable Map. Disponível em: https://www.submarinecablemap.com/. Acesso em: 15 de abr. de 2024.

Os provedores e operadoras utilizam também o IXPs (*Internet eXchange Points*) ou apenas IX que nada mais é que pontos de troca de tráfego, onde diferentes redes se encontram para trocar tráfego de *internet*. Isso ajuda a reduzir a latência e aumentar a eficiência e qualidade das comunicações online. Os IXPs são gerenciados por organizações neutras e independentes, que fornecem as instalações e os serviços necessários para facilitar a troca de tráfego entre os participantes. Como mencionam Tanenbaum e Wetherall (2011): “Um ISP pequeno poderia pagar a um ISP maior pela conectividade à *Internet* para alcançar hosts distantes, assim como um cliente compra o serviço de um provedor de *Internet*”.

Entretanto, para chegar ao usuário final, tem todo um caminho que o tráfego passa, onde se inicia na rede interna de um ISP que engloba as redes de acesso, que pode variar

dependendo da tecnologia de acesso à *internet* utilizada e da infraestrutura disponível na região. Como exemplo, temos, DSL (Digital Subscriber Line), Cabo *coaxial*, satélite é a fibra *óptica* que é considerada a mais utilizada atualmente.

Considerando a fibra *óptica* a tecnologia dominante em muitas redes de comunicação e buscando aprofundar um melhor entendimento sobre o funcionamento e sua distribuição, esse tipo de tecnologia geralmente utiliza-se como infraestrutura física: switches, OLT (*Terminal laser óptico*), Caixas de distribuição ou emenda, e às ONU(*Optical Network Unit*) ou ONT(*Optical Network Terminal*) que são os equipamentos alocados no usuário final.

Além dos componentes físicos, existem diversas configurações lógicas envolvidas na operação de uma rede que se estende até o cliente. Um exemplo disso são as configurações na OLT onde é necessário configurar os perfis que serão utilizados para cada tipo de serviço e assim coordenar o tráfego entre a rede e as ONUs/ONTs.

Para que haja a conexão entre duas ou mais pontas conectadas fisicamente é necessário a utilização de um switch para realizar o encaminhamento de pacotes através de vlan(Virtual Local Area *Network*) para tráfego e também para transporte de PPPOE(*Point-to-Point Protocol over Ethernet*) até algum autenticador local e logo para que possa ter a navegação é necessário que se tenha o roteamento estático ou dinâmico, no qual pode determinar qual o melhor o caminho que os dados trafegam na sua rede do início ao fim.

2.3 IMPORTÂNCIA DO MONITORAMENTO DE REDE.

Para manter a qualidade e acompanhar a nova era digital, os provedores de *Internet* enfrentam desafios significativos constantemente. Apesar de possuírem uma infraestrutura robusta para garantir a qualidade de seus serviços, é sabido que estão sujeitos a riscos e imprevistos. Há alguns anos, quando a tecnologia de fibra *óptica* era pouco conhecida, dominavam as conexões de *Internet* via satélite. Entretanto, essa opção é frequentemente criticada pelos usuários por ser mais propensa a interferências.

Já a fibra *óptica* é um tipo de tecnologia altamente confiável por ser resistente a interferências, garantindo uma conexão estável e de alta qualidade, capaz de suportar velocidades de transmissão de dados, além de oferecer baixa latência, tornando-a ideal para aplicações que demandam desempenho e confiabilidade, como redes corporativas e serviços de streaming de alta definição.

Outro desafio enfrentado pelos provedores de *internet* é o monitoramento da rede, pois não é apenas investir em uma infraestrutura como também é importante acompanhar o dia a dia para garantir a boa qualidade do serviço disponibilizado. O monitoramento de rede é uma estratégia abrangente para garantir a boa condição da rede, identificar possíveis gargalos, prevenir falhas e otimizar o desempenho de forma geral.

O autor Medrado (2018) destaca que o monitoramento da infraestrutura computacional se torna uma atividade fundamental para o funcionamento contínuo dos serviços oferecidos, garantindo a qualidade em níveis satisfatórios pelo maior tempo possível. Um dos principais problemas quando há falta de monitoramento é a incapacidade de detectar e solucionar problemas de forma ágil, o que leva a falhas na rede, lentidão e até mesmo indisponibilidade de serviços, o que muitas vezes só descobrem que existe uma falha quando gera um fluxo grande de reclamações dos clientes, o que gera grandes prejuízos tanto financeiramente como também da "reputação" do provedor.

Adotar um acompanhamento da rede em tempo real tende a prevenir e garantir a segurança em geral. No entanto, é fundamental atentar-se em como será esse monitoramento e quais as ferramentas serão utilizadas, visto que temos várias opções disponíveis atualmente, o que é necessário identificar quais atenderão melhor de acordo com as necessidades específicas de cada um. As principais ferramentas utilizadas incluem *Cacti*, *Nagios* e *Zabbix*. Além dessas, há também o *The Dude*, que embora não seja amplamente considerado como uma das principais ferramentas, destaca-se por sua facilidade de uso e é recomendado especialmente para provedores de pequeno porte.

2.4 PROTOCOLO

O monitoramento de redes ISP geralmente é realizado por meio de protocolos específicos, que permitem aos administradores coletar dados e identificar possíveis problemas, como congestionamentos, falhas de equipamentos ou ataques de segurança *Distributed Denial of Service* (DDosS) ou de forma geral os ataques cibernéticos. Além disso, a monitorização contínua da rede fornece informações valiosas que podem ser utilizadas para otimizar a infraestrutura e melhorar o desempenho geral, garantindo uma experiência de conectividade mais confiável para os clientes.

2.4.1 Protocolo SNMP

Um dos protocolos mais utilizados em monitoramento de rede é o *Simple Network Management Protocol* (SNMP), de acordo com o estudo do autor Daitx(2011) "A tecnologia SNMP é amplamente utilizada para o gerenciamento de redes. Este protocolo é uma alternativa natural de escolha para lidar com roteadores, quando considerados requisitos como operacionalidade, interoperabilidade e reuso." O SNMP tem várias vantagens, por isso é considerado um protocolo padrão de gerenciamento de rede.

O protocolo SNMP oferece diversas funcionalidades para o monitoramento e controle de dispositivos de rede. Algumas das principais funcionalidades do SNMP incluem a coleta de informações detalhadas através da comunicação no porta padrão 161 do protocolo *User Datagram Protocol* (UDP), na camada de aplicação do modelo *Open Systems Interconnection* (OSI). No SNMP, as informações são acessadas e manipuladas através do *Management Information Base* (MIB), que é uma estrutura hierárquica. O MIB define as variáveis gerenciadas disponíveis para monitoramento e controle. Algumas dessas informações incluem o estado do dispositivo, utilização de memória e *Central Processing Unit* (CPU), monitoramento do tráfego da rede, detecção de falhas em dispositivos de rede e taxa de erros de transmissão. Embora o SNMP possa ser usado para monitorar temperatura e voltagem em certos dispositivos de rede, esse tipo de monitoramento pode não ser suportado por todos os dispositivos.

O protocolo SNMP passou por mudanças ao longo dos anos, com o surgimento de novas versões que trazem melhorias. O SNMPv1 foi introduzido em 1988, estabelecendo as bases do protocolo. O SNMPv2 trouxe melhorias significativas, enquanto o SNMPv2c simplificou algumas funcionalidades. No entanto, foi com o SNMPv3, padronizado em 2002, que a segurança se tornou uma prioridade, com a inclusão de autenticação e criptografia robustas para proteger as comunicações SNMP contra acessos não autorizados e ataques maliciosos.

O SNMP é altamente escalável, o que significa que pode lidar com o crescimento da rede do provedor de *internet* sem comprometer o desempenho ou a eficácia do monitoramento. À medida que a infraestrutura de rede se expande para atender à crescente

demanda por serviços de *internet*, o SNMP pode ser facilmente configurado para incluir novos dispositivos e segmentos de rede. Essa flexibilidade e adaptabilidade fazem do SNMP uma ferramenta essencial para os provedores de internet que buscam manter uma operação eficiente e confiável em um ambiente em constante evolução.

2.4.2 Protocolo ICMP

Além do SNMP, outro protocolo comum usado para monitoramento de rede é o *Internet Control Message Protocol* (ICMP) que é uma abordagem para verificar a conectividade básica entre dispositivos de rede. Segundo os autores Jesus e Martins (2022) o ICMP é um protocolo da camada 3 do modelo ISO[2]/OSI (camada de Rede). É um protocolo utilizado para diagnósticos de problemas de comunicação de rede determinando a integridade e velocidade dos dados que estão chegando ao endereço destino.

O ICMP é o protocolo usado por ferramentas de diagnóstico de rede, como o comando "ping" no sistema operacional, para enviar mensagens de solicitação de eco (*echo request*) e receber respostas de eco (*echo reply*) dos dispositivos alvo. Essa troca de mensagens permite verificar a conectividade entre dispositivos de rede, sendo uma técnica fundamental para determinar se um dispositivo está acessível e se a comunicação está funcionando corretamente.

No entanto, no protocolo ICMP, sempre que uma resposta for recebida dentro de um tempo limite pré-definido e está correta, é um sinal claro de que o dispositivo está online e a conectividade está estabelecida. Por outro lado, se nenhuma resposta for recebida dentro do tempo limite especificado e a resposta recebida estiver incorreta, isso significa que há um problema de conectividade com o dispositivo. Este problema pode resultar por várias razões; por exemplo, falhas de rede, o dispositivo pode estar offline, ou roteamento apropriado uma vez que visto do diagrama. Como tal, é vital realizar uma revisão exaustiva para investigar o problema e abordá-lo apropriadamente.

ICMP pode ser uma ferramenta útil para identificar questões de rede, como congestionamento, falhas de hardware e problemas de conexão. É comum usar essa técnica como uma primeira avaliação para verificar se um dispositivo está acessível na rede. No entanto, é relevante notar que o monitoramento via ICMP não oferece informações detalhadas

[2] ISO-*International Organization for Standardization*

sobre o funcionamento interno dos dispositivos ou sobre o tráfego de rede. Seu uso principal é confirmar a disponibilidade básica dos dispositivos e identificar problemas de conectividade.

2.4.3 HTTP/HTTPS

O *Hypertext Transfer Protocol* (HTTP) foi criado em 1991 pela *European Organization for Nuclear Research* (CERN) como parte do projeto *World Wide Web*. Ele é o protocolo que possibilita a comunicação entre navegadores e servidores web, permitindo a troca de informações e a navegação na *internet*. Desde então, o protocolo evoluiu significativamente, passando por várias atualizações para melhorar sua eficiência, segurança e funcionalidade. Este protocolo opera seguindo um modelo de cliente-servidor, onde o cliente envia uma requisição a um servidor e este responde com os dados solicitados. Cada requisição HTTP é composta por um método, um *Uniform Resource Locator* (URL), e cabeçalhos que transmitem informações adicionais sobre a requisição.

Para melhorar a segurança nas comunicações, o HTTP *Secure*, conhecido como HTTPS, utiliza o protocolo SSL[3]/TLS[4] para criptografar a comunicação entre o cliente e o servidor. O HTTPS se tornou essencial para proteger dados sensíveis, como informações de login e transações financeiras contra-ataques maliciosos. Hoje, a adoção de HTTPS é amplamente incentivada, com navegadores modernos que informam e classificam como inseguros sites que não utilizam HTTPS, promovendo teoricamente um ambiente web mais seguro para todos os usuários.

O protocolo HTTP é a base da web, facilitando a troca de informações e a interação entre milhões de dispositivos conectados. Sua evolução reflete a necessidade de maior eficiência, segurança e capacidade de resposta às demandas crescentes da *internet* moderna. Além disso, o HTTP pode ser utilizado em ferramentas de monitoramento, que enviam requisições HTTP para verificar se um serviço *web* está funcionando corretamente.

---

[3] SSL-*Secure Sockets Layer*

[4] TLS-*Transport Layer Security*

3 METODOLOGIA

Para esta pesquisa, escolheu-se adotar uma metodologia de pesquisa descritiva para realizar uma análise comparativa das principais ferramentas de monitoramento, sendo escolhidos os softwares *Zabbix, Nagios e Cacti*. O objetivo principal deste estudo foi identificar e avaliar as características específicas e distintas de cada uma dessas plataformas, bem como seus desempenhos em ambientes operacionais em provedores de serviços de *internet*. Foi utilizado técnicas de revisão de literatura que permitem uma análise abrangente e imparcial das informações disponíveis.

A princípio, o processo metodológico consistiu na definição de critérios de seleção, os quais orientaram a escolha das fontes bibliográficas a serem consideradas. Alguns critérios foram estabelecidos com base na importância, atualidade e credibilidade das fontes consultadas, visando garantir a confiabilidade dos dados coletados. Além disso, foram consideradas as especialidades técnicas e operacionais de cada ferramenta, a fim de garantir uma comparação justa de cada uma delas.

Entretanto, após a definição dos critérios de seleção, buscou-se a realização de análise das literaturas disponíveis, utilizando-se periódicos especializados no tema, livros, artigos científicos, vídeos explicativos, manuais e documentos oficiais das próprias ferramentas e também outras fontes de pesquisa. Esta etapa envolveu a identificação e a seleção de técnicas que abordassem diretamente as funcionalidades, os recursos e os desempenhos das ferramentas em questão.

Após a coleta de informações, conduzimos uma análise dos dados utilizando técnicas de revisão da literatura. Essa etapa envolveu uma comparação crítica das características e desempenhos das ferramentas *Zabbix, Nagios e Cacti*, conforme os critérios estabelecidos anteriormente. Os resultados desta análise serão descritos de forma detalhada na seção de Resultados e Discussão, onde serão apresentados os quadros comparativos, gráficos e outras representações visuais para facilitar a interpretação.

Portanto, os resultados da análise foram avaliados considerando o conjunto de pesquisas atuais e os padrões emergentes no campo do monitoramento de redes. Foram identificadas as principais vantagens e desvantagens de cada ferramenta, assim como as áreas em que apresentam desempenho superior ou inferior em relação às demais.

4 RESULTADO E DISCUSSÃO

À medida que as redes de telecomunicações e demanda por conectividade se tornam cada vez mais presentes em nosso dia a dia, sabemos o quanto é essencial e necessário para os ISP realizar o monitoramento e acompanhamento da rede para garantir que os usuários finais recebam um serviço de qualidade. Nesta seção, vamos aprofundar se nos resultados de uma revisão completa das principais ferramentas e estratégias de monitoramento, sendo elas *Zabbix, Cacti e Nagios*. Ao analisarmos esses resultados em detalhes, poderemos entender melhor como as técnicas utilizadas contribuem para a operação eficiente, qualidade do serviço e a satisfação dos clientes.

4.1 CACTI

O *Cacti* é uma ferramenta de monitoramento de rede que permite coletar, armazenar e visualizar informações sobre o desempenho de uma rede de computadores. A coleta dos dados é realizada através do protocolo SNMP, e também permite algumas outras funções como criar gráficos e relatórios detalhados sobre o tráfego de rede e verificar a utilização de largura de banda. Com sua alta capacidade de visualização, o *Cacti* facilita aos administradores a identificação de problemas de funcionamento, o planejamento de atualizações de rede e a otimização da infraestrutura para atender às necessidades dos usuários finais.

Conforme Yano (2010, p.11), o *Cacti* oferece recursos importantes para o monitoramento de redes, ele monitora diversos itens como quantidade de memória utilizada, número de processos rodando, quantidade de usuários conectados, tráfego de entrada e saída, entre diversos outros, que podem variar de acordo com o tipo de dispositivo. Essa ferramenta é compatível com vários sistemas operacionais, como *Linux* e *Windows*, e seu manual de instalação, juntamente com as versões disponíveis, pode ser encontrado de forma gratuita no site oficial da plataforma, porém para sua instalação e utilização é preciso seguir alguns requisitos mínimos como apresentados no quadro 1:

Quadro 1 - Requisitos de *software* do *Cacti* (*Linux* e *Windows*)

Componente	**Linux**	**Windows**
Sistema Operacional	CentOS, Ubuntu, Debian, RHEL, entre outros	Windows 7, 8, 10, Server 2008, 2012, 2016, 2019
Servidor Web	Apache	Apache ou IIS
PHP	PHP 7.x ou superior	PHP 7.x ou superior
Banco de Dados	MySQL ou MariaDB	MySQL ou MariaDB
RRDtool	N/A (depende da instalação do Cacti)	N/A (depende da instalação do Cacti)
Requisitos de Hardware	RAM: mínimo de 2 GB; Processador: 1 GHz ou superior; Espaço em Disco: mínimo de 5 GB;Conectividade de Rede	RAM: mínimo de 2 GB; Processador: 1 GHz ou superior; Espaço em Disco: mínimo de 5 GB; Conectividade de Rede

Fonte: Autoria própria (2024).

No trabalho realizado por Silva e Sousa (2019) foi utilizado o Cacti em equipamentos de baixa demanda de recursos para monitoramento de redes. Para utilização da ferramenta de monitoramento o autor escolheu a versão 0.8.8f do *Cacti*, utilizou a máquina virtual (VM) *VirtualBox* com sistema operacional *Ubuntu* 16.04 *server* e o *software* PHP[5] *Network Weathermap* que é utilizado para criar mapas de rede dinâmicos que exibem informações de forma visual. Uma observação foi que a versão escolhida pelos pesquisadores apresentou erros nas permissões onde os mesmos realizaram a correção. Foi monitorado algumas características como espaço usado no Disco Local C, uso da CPU e o tráfego de dados no adaptador wireless de dispositivos nomeados como “dispositivos clientes”, para os quais foi preciso habilitar o protocolo SNMP para fins de monitoramento. Em conclusão dos autores o uso do *Cacti*, em conjunto com seu plugin *Weathermap*, ofereceu uma solução eficiente e um bom desempenho para monitorar redes, independentemente da sua complexidade. No entanto, ele observa que o processo de adequação de equipamentos para o monitoramento de redes

[5] PHP-*Hypertext Preprocessor*

pode ser viável, mas apresenta desafios, como a possibilidade de instabilidade e erros durante a configuração do *firmware*.

No estudo de Medrado (2018), foi realizado um caso prático sobre o uso de soluções de monitoramento em um ambiente de data center. Neste trabalho foi utilizado o sistema operacional Linux *Debian* 9 e instalado a versão 0.8.8 do *Cacti* e o *plugin* PHP *Network Weathermap.* O autor apresentou um manual detalhado de instalação da ferramenta de monitoramento e de todos os seus requisitos, onde durante a instalação não apresentou nenhuma falha, Foi também realizado cadastro de 182 hosts que foram as bases para análise da ferramenta. Em conclusão, o autor observou que o Cacti teve um bom desempenho e cumpriu com seu papel. Foi empregado para gerar uma variedade de gráficos que, aliados ao *plugin* PHP *Network Weathermap*, proporcionaram uma representação em tempo real do uso dos links de dados entre os equipamentos monitorados. Desde a sua instalação até a utilização, não foi registrada nenhuma falha que pudesse causar problemas ou alguma desvantagem.

Em outra pesquisa realizada por Alves Junior (2020) onde foi implantado o cacti para o gerenciamento de redes de computadores em uma máquina virtual. A versão do *Cacti* utilizada foi 1.2.10 (versão mais recente quando foi desenvolvido o trabalho) a máquina virtual foi a Oracle VM *VirtualBox*, o sistema operacional escolhido foi *Debian* versão 10.2.0 e neste caso utilizou-se também o GNS3[6] versão 2.2.5 que é uma plataforma de simulação de redes de código aberto que permite aos usuários modelar, configurar e testar redes virtuais. Seguindo ainda as análises e perspectivas do autor, temos também os requisitos para utilização do GNS3 apresentados no quadro 2.

Quadro 2 - Requisitos de hardware GNS3

[6] GNS3-*Graphical Network Simulator*-3

ITEM	REQUISITO
SO	Windows 7 (64 bit) or later.
Processador	2 ou mais núcleos lógicos.
Virtualização	Extensões de virtualização necessárias. Pode ser necessário habilitá-lo através do BIOS do seu computador.
Memória	4 GB RAM.
Armazenamento	1 GB de espaço disponível.
Notas adicionais	Pode ser necessário armazenamento adicional para o sistema operacional e as imagens do dispositivo.

Fonte: Autoria própria.

Fonte: Alves Junior (2020, p. 19).

Após todo o processo de preparação da máquina virtual e instalação do *Cacti*, o analista prosseguiu para a fase de testes básicos. Para isso foram configurados o roteador, o servidor SNMP e o cliente SNMP. Não foram registrados problemas durante o processo de instalação e teste, e também não foi demonstrado nenhum grau de dificuldade significativo. O autor conclui que alcançou com sucesso o objetivo básico e destaca a integração do GNS3, que facilita os testes antes da implantação em uma rede real. Embora não tenham sido realizados testes, foi mencionada a disponibilidade de uma ampla variedade de extensões (*plugins*) para monitorar diversos parâmetros da rede utilizando o Cacti.

4.2 NAGIOS

O *Nagios* é uma ferramenta de código aberto de monitoramento muito utilizada e conhecida por sua eficácia em manter a integridade e disponibilidade da infraestrutura de redes. Criado por *Ethan Galstad* em 1999, inicialmente chamado de *Netsaint*, o *Nagios* rapidamente se tornou uma referência no setor tecnológico devido à sua capacidade de monitorar servidores, redes e serviços em tempo real. Com uma interface web intuitiva, fornece uma visão abrangente do estado da infraestrutura o que permite a detecção rápida de problemas e a solução de problemas antes que afetem os usuários finais.

Segundo Gaia (2019), o *Nagios* é descrito como "um software robusto, porém com uma alta curva de aprendizagem que pode dificultar a utilização de todas as suas funções. Possui a habilidade de integrar-se a tecnologias já existentes por possuir muitos complementos sob a licença GPL, que estendem a sua capacidade". O *Nagios* não tem restrição quanto aos sistemas operacionais e pode ser instalado no *Linux* (como *CentOS*, *Ubuntu*, *Debian*, etc.) e *Unix* (como FreeBSD). Também é possível instalá-lo em sistemas

Windows, mas geralmente é mais comum em ambientes *Linux*/*Unix*. Para sua utilização é necessário seguir seus requisitos para obter um bom funcionamento, vejamos no quadro 3.

Quadro 3 - Requisitos de *software* do *Nagios (Linux e Windows)*.

Componente	**Linux**	**Windows**
Sistema Operacional	Ubuntu, Debian, CentOS, Fedora, openSUSE, entre outros	Windows 8.1, 10, Server 2012, 2012 R2, 2016, 2019
Servidor Web	Apache HTTP Server ou Nginx	Apache HTTP Server (ou IIS)
Banco de Dados	Opcional (ex: MySQL, PostgreSQL) somente para componentes adicionais como o Nagios XI	Opcional (ex: MySQL, PostgreSQL) somente para componentes adicionais como o Nagios XI
Requisitos de Hardware	RAM: 1GB-2GB; Processador: 1GHz+; Espaço em Disco: Algumas dezenas de GB ;Conectividade de Rede	RAM: 1GB-2GB; Processador: 1GHz+; Espaço em Disco: Algumas dezenas de GB.

Fonte: Autoria própria (2024).

Entretanto, esses são os principais componentes e requisitos necessários para instalar o *Nagios* em sistemas *Linux* e *Windows*. É importante lembrar que esses são requisitos gerais e podem variar dependendo do tamanho e da complexidade da infraestrutura de monitoramento importante também consultar a documentação específica do *Nagios* para obter instruções detalhadas sobre como configurar o *Nagios* em cada ambiente específico.

Fornaroli e Alves (2021) realizaram um trabalho utilizando o *Nagios* para monitorar a saúde de serviços, sistemas e dispositivos de rede. Para tal, foi utilizado o sistema operacional *CentOS* e descrito todo processo de instalação e preparação da ferramenta. No diagnóstico e resultados o analista destacou os diferentes estados que podem ocorrer durante o processo que ajuda no entendimento do diagnóstico da rede, onde é possível identificar quando algo não está funcionando corretamente e também quando está inoperante. Em destaque nas considerações finais o *Nagios* foi considerado bem flexível desde sua instalação e configuração até sua utilização para monitoramento, foi considerado também uma ferramenta

de qualidade permitindo o controle preciso dos ativos tecnológicos e a tomada de decisões estratégicas.

Conforme o estudo de Barros e Tavares (2021), para aprimorar a segurança de sistemas baseados no protocolo SNMP contra-ataques de negação de serviço, os autores utilizaram o *Nagios* para provar que mesmo com uma ferramenta de monitoramento podem ocorrer ataques DDoS na rede. Para este trabalho, eles utilizaram a ferramenta em um ambiente virtual e simularam um ataque em um host, em um dos testes os pesquisadores identificaram que o *Nagios* utiliza o protocolo SNMP para gerenciamento, operando nas portas padrão 161 e 162 eles então sobrecarregaram a porta 162 com excesso de pacotes enviados, onde conseguiram interromper o gerenciamento da rede pelo *Nagios*. Em conclusão, os autores destacam que o *Nagios* é limitado referente suas configurações padrão, o que é necessário a incorporação de recursos adicionais para garantir sua segurança. Nesse sentido, cabe ao administrador buscar alternativas em termos de mecanismos de segurança para manter o funcionamento adequado da rede.

No trabalho de Braga (2019), foram avaliadas algumas ferramentas de monitoramento em sistemas de alta disponibilidade. Uma das ferramentas escolhidas foi o *Nagios* e o *Zabbix*, nos quais o autor realizou uma comparação entre eles. Foi utilizado o sistema operacional *Linux* CentOS 7, juntamente com o Data *Replicator Block Device* (DRBD), que é uma tecnologia de *software* que replica dados em tempo real entre as máquinas. O autor ainda ressalta uma observação a respeito desta ferramenta, que é a configuração padrão de monitoramento contínuo, sendo de 24 horas por dia durante 30 dias. Dependendo do que está sendo monitorado, os resultados podem não representar com precisão a realidade desejada. Na comparação realizada entre o *Nagios* e o *Zabbix*, o autor descreve que o *Nagios* apresenta um desempenho inferior devido ao *hardware* e ao seu banco de dados interno, o que deixou a máquina com uma lentidão exagerada, dificultando também a utilização da interface gráfica. O pesquisador ressalta também que essa desvantagem sobre o *Nagios* é válida apenas para seu estudo realizado, que foi uma comparação simples, e mesmo com essas análises, ainda continua sendo recomendado para utilização.

4.3 ZABBIX

O *Zabbix* é amplamente reconhecido como um dos principais *softwares* de monitoramento de redes, ocupando a posição de liderança no mercado. Foi desenvolvido por *Alexei Vladishev* em 1998 como uma solução interna enquanto ele trabalhava em um provedor de *internet*. De acordo com Silva, Martins e Medeiros (2015), a utilização do *Zabbix* possibilita os profissionais de tecnologia operar o Centro de Gerenciamento de Redes (CGR) por meio de alarmes em tempo real, que podem ser enviados via *e-mail* e mensagens de texto através de aplicativos como *WhatsApp* e *Telegram*.

Por outro lado, Luiz Mariano do Vale (2017) destaca que a interface *web* do *Zabbix* permite ativar alertas sonoros em caso de incidentes, além de oferecer recursos para visualização de painéis de controle, gráficos, mapas e telas com informações sobre o status e desempenho dos itens monitorados. Os autores ainda ressaltam que mesmo a ferramenta sendo de código aberto, possui suporte comercial e apenas um único servidor *Zabbix* é capaz de fazer o monitoramento de até 25000 *hosts*.

O *Zabbix* é oferecido gratuitamente, mas existe uma versão paga destinada ao uso corporativo, especialmente para aqueles que necessitam de suporte garantido e serviços adicionais como as empresas ISP. Antes de sua utilização, é crucial verificar os requisitos de *hardware* e *software* para garantir uma instalação bem-sucedida e um bom desempenho. Essas especificações estão detalhadas no quadro 4.

Quadro 4 - Requisitos de *software* do Nagios (*Linux* e *Windows*).

Componente	**Linux**	**Windows**
Sistema Operacional	CentOS, Ubuntu, Debian, RHEL, entre outros	Windows 7, 8, 10, Server 2008, 2012, 2016, 2019
Servidor Web	Apache	Apache ou IIS
PHP	PHP 7.x ou superior; Extensões PHP necessárias: mysqli, gd, libxml, bcmath, ctype, gettext, xmlreader, mbstring, sockets	PHP 7.x ou superior; Extensões PHP necessárias: mysqli, gd, libxml, bcmath, ctype, gettext, xmlreader, mbstring, sockets

Continua...

Banco de Dados	MySQL, MariaDB, PostgreSQL, SQLite, Oracle, IBM Db2	MySQL, MariaDB, PostgreSQL, SQLite, Oracle, IBM Db2
Requisitos de Hardware	RAM: mínimo de 2 GB; Processador: 1 GHz ou superior; Espaço em Disco: mínimo de 20 GB; SSD recomendado; Conectividade de Rede	RAM: mínimo de 2 GB; Processador: 1 GHz ou superior; Espaço em Disco: mínimo de 20 GB; SSD recomendado; Conectividade de Rede

Fonte: Autoria própria (2024).

No estudo de caso conduzido pelos autores Silva e Silva (2024), foi implementado o *Zabbix* para o monitoramento da rede de dados. A instalação da ferramenta ocorreu em uma máquina virtual *VirtualBox*, seguindo as instruções disponíveis no site oficial em português. O sistema operacional escolhido foi o *Ubuntu* versão 20.04 de 64 bits, e a versão do *Zabbix* utilizada foi a 6.09 LTS[7], com o banco de dados *MySQL* e o servidor *web Nginx*.

Durante o processo de instalação dos clientes remotos, os autores encontraram dificuldades devido às falhas na obtenção das informações de monitoramento, decorrentes da separação das redes. Para solucionar esse problema, foi necessário configurar uma VPN (*Virtual Private Network*), utilizando a ferramenta *Hamachi*, conhecida por suas interfaces gráficas intuitivas que facilitam a configuração e utilização. Os autores observaram também que, embora o *Zabbix* seja uma ferramenta eficiente, não atendia completamente às necessidades de visualização de dados através de dashboards. Como solução, escolheram integrar o Grafana, uma ferramenta de código aberto e gratuita desenvolvida para a visualização e análise de dados. Apesar da necessidade de adotar outra plataforma para a parte gráfica e de dashboards, os autores concluíram que os objetivos pretendidos com a utilização do *Zabbix* foram alcançados. No entanto, ressaltaram a importância de aprimorar as configurações de acordo com as especificidades de cada cliente.

O autor Bueno (2022) realizou um estudo sobre o monitoramento de rede utilizando o *Zabbix*, complementado pelo Grafana para integrar e visualizar os resultados obtidos. Para esta experiência, utilizamos o sistema operacional *Ubuntu* e a versão 6.0.7 do *Zabbix* para instalação foi utilizado a documentação oficial contendo o passo a passo de cada processo. A

[7] LTS-*Long-term support*

pesquisa foi conduzida em um ambiente doméstico, monitorando os seguintes dispositivos: 1 notebook, 1 *desktop*, 5 celulares e 1 *Smart* TV. O processo de instalação das ferramentas foi realizado sem dificuldades. Em conclusão, o autor destaca que o *Zabbix* e o Grafana simplificam o monitoramento de redes, graças às *dashboards* intuitivas e alertas automáticos. O *Zabbix* mostrou-se versátil e fácil de configurar, com um tema padrão que atende à maioria dos dispositivos, embora modelos específicos possam ser necessários para informações detalhadas. Mesmo em um ambiente doméstico, essas ferramentas demonstraram grande eficácia e têm potencial significativo para uso corporativo.

No projeto realizado por Calú et al. (2020), o *Zabbix* foi implementado para monitoramento no câmpus Arapiraca da Universidade Federal de Alagoas. A escolha dessa ferramenta se deve ao fato de ser considerada uma das mais completas e eficientes no mercado. Para a implantação do *Zabbix*, ele foi instalado em uma máquina virtual utilizando o sistema operacional *Debian* 10, com as seguintes configurações de *hardware*, entre outras: memória RAM de 8GB e 4 processadores *Common* KVM com frequência de 2000 MHz. Após a configuração da ferramenta, os autores iniciaram o processo de testes e implantação, onde foi possível analisar CPU, temperatura dos dispositivos, perda de pacotes do link principal, consumo de *internet* e também a organização de toda a estrutura da rede através de mapeamento. Em conclusão, após obter ótimos resultados com a implantação da ferramenta de monitoramento na Universidade Federal de Alagoas (UFAL), descartando até a possibilidade de aumento da banda larga contratada, os autores destacam que o *Zabbix* cumpre com as necessidades e se mostra eficiente para gerenciamento, além de oferecer baixo custo, boa usabilidade e várias funcionalidades. Isso permite identificar, visualizar, corrigir, antecipar e prevenir problemas de rede, melhorando a qualidade dos serviços.

4.4 ANÁLISE COMPARATIVA DE SISTEMAS DE MONITORAMENTO: CACTI, NAGIOS E ZABBIX

Os sistemas de monitoramento de rede, como *Cacti*, *Nagios* e *Zabbix*, são amplamente utilizados para garantir a disponibilidade e o desempenho das infraestruturas em provedores de serviços de *internet*. Cada uma dessas ferramentas possui características, vantagens e desvantagens específicas, tornando-as mais adequadas para diferentes cenários de uso.

Durante as pesquisas, constatou-se que o *Cacti*, apesar de suas funcionalidades, apresentou problemas de permissões que exigiram correções. O *Nagios*, embora eficiente, requer a adição de recursos extras para superar limitações de segurança em sua configuração padrão. Por fim, o *Zabbix* demonstrou a falta de funcionalidades avançadas para visualização de dados, o que levou à integração do Grafana como solução complementar. Dessa forma, a escolha da ferramenta ideal depende da adaptação às necessidades específicas de cada ambiente e das soluções implementadas para contornar eventuais limitações.

- *Cacti*

O *Cacti* é conhecido por sua capacidade de criar gráficos detalhados e relatórios de desempenho da rede. Ele utiliza o protocolo SNMP para coletar dados e é amplamente utilizado para monitorar a utilização da largura de banda, tráfego de rede e outros parâmetros de desempenho. A interface web do *Cacti* é intuitiva e facilita a criação de gráficos e visualização de dados.

- *Nagios*

O *Nagios* é uma ferramenta de monitoramento robusta e altamente configurável, capaz de monitorar uma vasta gama de serviços e dispositivos. Desenvolvido inicialmente como *Netsaint*, o *Nagios* tem uma curva de aprendizado mais acentuada devido à sua complexidade, mas oferece uma grande flexibilidade através de seus complementos e plugins. Ele é capaz de enviar alertas em tempo real via e-mail e outras notificações, permitindo uma rápida resposta a problemas.

- *Zabbix*

O *Zabbix* é considerado uma das ferramentas de monitoramento mais completas e eficientes no mercado. Ele oferece monitoramento em tempo real, alertas avançados, visualização de dados e suporte a diversos tipos de dispositivos e serviços. O *Zabbix* também possui uma interface *web* robusta que permite a criação de dashboards personalizados. Além disso, sua capacidade de monitorar até 25.000 hosts com um único servidor o torna uma escolha poderosa para grandes infraestruturas.

No quadro 5 podemos observar a comparação de cada ferramenta de acordo com alguns critérios.

Quadro 5. Comparação de ferramentas de monitoramento.

Característica	Cacti	Nagios	Zabbix
Ano de Criação	2001	1999	1998
Desenvolvedor	Ian Berry	Ethan Galstad	Alexei Vladishev
Uso Principal	Coleta e visualização de dados de desempenho	Monitoramento de serviços e dispositivos	Monitoramento completo e análise de desempenho
Protocolos Suportados	SNMP, ICMP	SNMP, NRPE, NCPA, entre outros	SNMP, IPMI, JMX, entre outros
Interface Web	Sim	Sim	Sim
Curva de Aprendizado	Moderada	Alta	Moderada
Alertas em Tempo Real	Não	Sim	Sim
Escalabilidade	Moderada	Alta	Alta
Requisitos de Hardware	Baixos	Moderados a altos	Moderados a altos
Sistema Operacional	Linux, Windows	Linux, Unix, Windows	Linux, Unix, Windows
Suporte Comercial	Não	Sim	Sim
Funcionalidades Adicionais	Gráficos detalhados e relatórios	Monitoramento extensível com plugins	Dashboards personalizados e análise preditiva
Código Aberto	Sim	Sim	Sim
Requisitos Mínimos	RAM: 2 GB; CPU: 1 GHz	RAM: 1-2 GB; CPU: 1 GHz+	RAM: 2 GB; CPU: 1 GHz+

Fonte: Autoria própria (2024).

A escolha entre os três subtemas de monitoramento dependerá das necessidades específicas de cada ocasião e também da infraestrutura existente ou que o usuário pretende implementar. O *Cacti* é excelente para visualização detalhada de dados e é relativamente fácil de configurar. Já o *Nagios* oferece muitas opções e é resistente, sendo ideal para monitorar uma grande variedade de serviços e dispositivos. *Zabbi*x, por outro lado, fornece uma solução completa com capacidades avançadas de monitoramento, capacidade de crescimento e visualização, sendo uma excelente escolha para grandes infraestruturas.

5 PROPOSTA DE IMPLEMENTAÇÃO DE SISTEMA DE MONITORAMENTO PARA MELHORIA DA INFRAESTRUTURA DE REDE NO IF SUDESTE MG CÂMPUS AVANÇADO BOM SUCESSO.

O Instituto Federal Sudeste de Minas Gerais (IF Sudeste MG), Câmpus Avançado Bom Sucesso, desempenha um papel fundamental no avanço educacional e desenvolvimento tanto da cidade quanto da região, oferecendo cursos de graduação, técnicos e de Formação Inicial e Continuada (FIC). Desde o início de suas atividades acadêmicas em 2012, a instituição está em constante evolução tecnológica e teve uma precisão mais significativa após a pandemia de COVID-19, que exigiu por si a transição temporária para o ensino à distância.

Com o retorno das aulas presenciais em 2022, houve a necessidade de adaptação e melhoramento da infraestrutura de rede da instituição devido à experiência durante 2 anos de ensino remoto, a qual todos os envolvidos utilizaram intensivamente recursos tecnológicos no dia a dia. Diante desse cenário, foram implementadas melhorias na infraestrutura de rede, bem como aprimoramentos na administração e distribuição por toda a área da instituição. Apesar das medidas tomadas anteriormente, estas não foram suficientes, levando a uma reestruturação da rede interna como parte da atual reforma, visando atender de maneira mais eficaz às demandas tecnológicas e administrativas.

Nesse contexto, considerando a complexidade crescente das operações e a necessidade de manter uma rede estável e segura, surge a proposta de implantar um sistema de gerenciamento de rede. Esta iniciativa não só irá facilitar o trabalho do departamento de TI, permitindo monitoramento contínuo e intervenção proativa em eventuais falhas, como também proporcionará recursos para melhorar continuamente a infraestrutura tecnológica do instituto.

Para viabilizar essa reestruturação, é importante realizar um levantamento detalhado dos recursos existentes e das necessidades específicas de cada setor, incluindo a contagem das salas de aula disponíveis, a quantidade de computadores nos laboratórios de informática, assim como a identificação das salas administrativas (como secretaria, biblioteca, sala dos professores, administrativos e TI). Além disso, é essencial avaliar a cobertura e a capacidade do acesso *Wi-Fi* disponível para alunos e professores em todo o câmpus.

Para suportar eventos especiais que exigem uma infraestrutura adicional, será necessário planejar uma estratégia que permita escalabilidade e flexibilidade. Isso pode

envolver a implementação de pontos de acesso temporários ou o reforço da capacidade existente, garantindo que eventos de grande porte sejam apoiados por uma infraestrutura de rede confiável e eficiente.

Ao finalizar esse levantamento detalhado e implementar as melhorias necessárias, a instituição estará preparada não apenas para enfrentar os desafios atuais, mas também para se adaptar às necessidades futuras de tecnologia e conectividade no ambiente educacional.

6 CONSIDERAÇÕES FINAIS

Durante a análise detalhada dessas ferramentas, ficou evidente que cada uma delas possui características únicas que as tornam adequadas para diferentes necessidades e contextos. O *Cacti*, com sua interface intuitiva e foco em gráficos detalhados, é ideal para monitoramento de desempenho visual. O *Nagios*, com sua flexibilidade e variedade de plugins, é indicado para ambientes que requerem monitoramento extensivo e notificações em tempo real. Já o *Zabbix* se destaca por seu eficiente desempenho e funcionalidades avançadas como gráficos e relatórios, sendo uma excelente opção para grandes infraestruturas que demandam monitoramento em tempo real e análise preditiva.

Ao observar os trabalhos e artigos sobre as principais ferramentas de monitoramento de rede *Cacti*, *Nagios* e *Zabbix*, podemos concluir que este trabalho cumpriu sua proposta de analisar e destacar as capacidades de cada software, observando suas funcionalidades e aplicações. Considerando que atualmente estamos vivenciando um cenário marcado pela evolução digital e pelo aumento da demanda por conectividade, a escolha e implementação eficaz desses *softwares* são importantes para garantir a qualidade operacional das redes e também a qualidade de serviços e gerenciamento relacionados ao departamento de TI[8].

Além de identificar as capacidades dessas ferramentas, o trabalho também demonstrou que as ferramentas de monitoramento podem ser utilizadas não somente por operadoras e provedores como também instituições ou empresas de pequeno e grande porte para aprimorar a qualidade de seus serviços, garantindo uma resposta rápida a falhas e, consequentemente, elevando a excelência operacional em um cenário de crescente demanda por conectividade.

Em suma, o resultado desta revisão teórica cumpriu o objetivo de contribuir para o auxílio na identificação da melhor ferramenta de monitoramento, destacando que a escolha ideal é aquela que melhor atende às necessidades específicas do usuário. O quadro 4, apresentado no tópico 4.4, oferece um guia básico e prático para orientar profissionais do setor na seleção e implementação das ferramentas de monitoramento mais adequadas.

[8] TI-Tecnologia da Informação

REFERÊNCIAS

ALVES JUNIOR, Alsemiro. **Gerenciamento de redes de computadores utilizando CACTI**: um exemplo em ambiente virtual**.** 2020. Trabalho de Conclusão de Curso (Especialização em Configuração e Gerenciamento de Servidores e Equipamentos de Redes) – Universidade Tecnológica Federal do Paraná, Curitiba, 2020. Disponível em: http://repositorio.utfpr.edu.br/jspui/handle/1/29916. Acesso em: 28 abr. 2024.

BARROS, E. G.; TAVARES, J. L. Melhorando a segurança de sistemas baseados no protocolo SNMP contra-ataques de negação de serviço (DOS). **Monumenta** - Revista Científica Multidisciplinar, v. 2, n. 2, p. 1–4, 2021. Disponível em: https://revistaunibf.emnuvens.com.br/monumenta/article/view/24. Acesso em: 28 abr. 2024.

BRAGA, Francisco José de Luccas. **Avaliando ferramentas de monitoramento em sistemas de alta disponibilidade.** 2019. Trabalho de Conclusão de Curso (Graduação em Tecnologia em Sistemas de Computação) - Instituto de Computação, Universidade Federal Fluminense, Niterói, 2019. Disponível em: https://app.uff.br/riuff/handle/1/30824. Acesso em: 7 maio 2024.

DAITX, Fábio Fabian. **Uma solução baseada em SNMP para gerenciamento de dispositivos de rede com suporte à virtualização.** Dissertação (Mestrado em Ciências da Computação) - Universidade Federal do Rio Grande do Sul, Instituto de Informática, Porto Alegre, 2011. Disponível em: https://lume.ufrgs.br/bitstream/handle/10183/34806/000788650.pdf. Acesso em: 10 abr. 2024.

FUNDACÃO BRADESCO. **Internet**: virtual vision 6.0. 2010. Disponível em: https://www.ev.org.br/static/acessibilidade/files/Internet_6.pdf. Acesso em: 07 jun. 2024.

GAIA, Danilo Silvio. **Monitoramento de redes com Nagios**: monitoramento em central de recepção, processamento e retransmissão de sinais de vídeo e internet em rede HFC. 2019. 44 p. Trabalho de Conclusão de Curso (Graduação em Engenharia Elétrica) – Faculdade Anhanguera de Piracicaba, Piracicaba. Disponível em: https://repositorio.pgsscogna.com.br/bitstream/123456789/23604/1/DANILO%20SILVIO%20GAIA.pdf. Acesso em: 28 abr. 2024.

JESUS, V. R. S.; MARTINS, G. H. **Tecnologias e monitoramento em redes de computadores**: implementação de tecnologias e exploração de recursos de monitoramento. 2022. Trabalho de Conclusão de Curso (Tecnólogo em Redes de Computadores) - Faculdade de Tecnologia FATEC Bauru. Orientador: Martins, H. P. Disponível em: http://ric.cps.sp.gov.br/handle/123456789/11248. Acesso em: 15 abr. 2024.

KUROSE, J. F.; ROSS, K. W. **Redes de computadores e a Internet**: uma abordagem top-down. 6. ed. São Paulo: Pearson, 2013.

VALE, Luiz Mariano do. **Monitoramento de redes**: a importância do monitoramento de redes para a segurança da informação. 2017. Estudo de caso (Gestão da Tecnologia da Informação) – Universidade do Sul de Santa Catarina, Santa Catarina, 2017.

MEDRADO, Rainer Testa. **Monitoramento de ativos de rede utilizando softwares open-source.** 2018. Monografia (Especialização em Configuração e Gerenciamento de Servidores e Equipamentos de Redes) - Departamento Acadêmico de Eletrônica, Universidade Tecnológica Federal do Paraná, Curitiba, 2018. Disponível em: http://repositorio.utfpr.edu.br:8080/jspui/bitstream/1/17218/1/CT_GESER_X_2018_07.pdf. Acesso em: 07 abr. 2024.

GERENCIAMENTO de cadeia de suprimentos: internet das coisas**.** c2022. Disponível em: https://www.oracle.com/br/internet-of-things/what-is-iot/. Acesso em: 26 abr. 2022.

MELO, Paulo Roberto de Sousa; GUTIERREZ, Regina Maria Vinhais. A Internet e os provedores de acesso**. BNDES Setorial**, Rio de Janeiro, n. 10, p. 115-172, set. 1999. Disponível em: https://web.bndes.gov.br/bib/jspui/bitstream/1408/8559/2/BS%2010%20A%20Internet%20e%20os%20Provedores%20de%20Acesso_P_BD.pdf. Acesso em: 19 mar. 2024.

SANTOS, Bruno P. *et al.* **Internet das coisas**: da teoria à prática**.** Departamento de Ciência da Computação, Universidade Federal de Minas Gerais. Belo Horizonte, MG, Brasil, 2024.

SILVA, Wagner José da; SILVA, Roger Assunção da. Implementação de monitoramento de rede de dados com Zabbix e Grafana: um estudo de caso. **P2P e Inovação**, v. 10, n. 2, abril 2024. DOI: 10.21728/p2p.2024v10n2e-6904. Disponível em: https://www.researchgate.net/publication/380230043_IMPLEMENTACAO_DE_MONITORAMENTO_DE_REDE_DE_DADOS_COM_ZABBIX_E_GRAFANA_um_estudo_de_caso. Acesso em: 15 abr. 2024.

SILVA, Andreiver Mateus Ferreira; SOUSA, Sérgio Barros de. **Monitoramento de redes utilizando Cacti e PHP Weathermap em equipamentos de baixa demanda de recursos.** Disponível em: http://repositorio.uespi.br:8080/handle/123456789/156. Acesso em: 28 abr. 2024.

SILVA, Antonio Vinicius Ferreira e. **Uma análise comparativa das versões do protocolo HTTP**: evolução e pontos que ampliem o uso do HTTP/3**.** 2021. Trabalho de Conclusão de Curso (Graduação em Sistemas de Informação) - Centro Universitário Christus (Unichristus), Fortaleza, 2021. Disponível em: https://repositorio.unichristus.edu.br/jspui/bitstream/123456789/1175/1/TCC%20-%20Antonio%20Vinicius%20Ferreira%20e%20Silva.pdf. Acesso em: 10 jul. 2024.

SUBMARINE CABLE MAP. **Submarine cable map.** Disponível em: https://www.submarinecablemap.com/. Acesso em: 15 abr. 2024.

UMA, Eduardo. **Trabalho, Tecnologia e Desemprego.** 2. ed. São Paulo: Grupo Almedina, 2022. *E-book*. Disponível em: https://app.minhabiblioteca.com.br/reader/books/9786556277028/. Acesso em: 15 abr. 2024.

YANO, Inácio Henrique. **Gerenciamento de redes de computadores utilizando CACTI.** Campinas: Embrapa Informática Agropecuária, 2010. Disponível em: https://www.infoteca.cnptia.embrapa.br/bitstream/doc/883562/1/doc10510.pdf. Acesso em: 10 abr. 2024.