PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS

ESCOLA POLITÉCNICA E DE ARTES

GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

GRAFANA COMO UMA FERRAMENTA DE VISUALIZAÇÃO DE MONITORAMENTO DE REDES DE COMPUTADORES

GABRIEL DE CASTRO GONÇALVES

GOIÂNIA

2024

GABRIEL DE CASTRO GONÇALVES

GRAFANA COMO UMA FERRAMENTA DE VISUALIZAÇÃO DE MONITORAMENTO DE REDES DE COMPUTADORES

Trabalho de Conclusão de Curso apresentado à Escola Politécnica e de Artes, da Pontifícia Universidade Católica de Goiás, como parte dos requisitos para obtenção do título de Bacharel em Ciência da Computação. Orientador:
Profa. Dra. Solange da Silva
Banca examinadora:
Prof. Dr. Fabio Barbosa Rodrigues
Prof. Me. Wilmar Oliveira de Queiroz

GOIÂNIA

2024

GABRIEL DE CASTRO GONÇALVES

MONITORAMENTO DE REDES DE COMPUTADORES UTILIZANDO GRAFANA

Trabalho de Conclusão de Curso aprovado em sua forma final pela Escola Politécnica e de Artes, da Pontifícia Universidade Católica de Goiás, para obtenção do título de Bacharel em Ciência da computação, em 18/06/2024.

_____

Orientadora Prof.ª Dra. Solange da Silva

_____

Prof. Me. Wilmar Oliveira de Queiroz

_____

Prof. Dr. Fábio Barbosa Rodrigues

GOIÂNIA,

2024

AGRADECIMENTOS

Agradeço do fundo do meu coração a Deus por sua presença constante nos momentos desafiadores da minha vida.

Quero expressar minha profunda gratidão aos meus pais por tornarem possível minha jornada de graduação na PUC GO. Agradeço ao meu pai por sua inabalável confiança em minhas escolhas ao longo dessa jornada e à minha mãe por seu apoio incondicional, sempre me acolhendo nos momentos de dificuldade e reforçando minha capacidade, e à minha namorada por seu constante apoio. Suas presenças foram fundamentais em minha trajetória.

Minha gratidão se estende à minha orientadora, Solange da Silva, pela sua incrível paciência, dedicação e orientação valiosa neste TCC, trabalhando lado a lado comigo em busca do sucesso.

Não posso deixar de agradecer a todos os meus professores durante minha graduação e a todas as pessoas que, de diversas maneiras, contribuíram para o desenvolvimento deste trabalho. Seu apoio e conhecimento foram fundamentais para o alcance deste objetivo.

RESUMO

Este trabalho tem como objetivo geral desenvolver um estudo da ferramenta Grafana para descrever seu funcionamento e mostrar como seu uso facilita a interpretação e a compreensão dos dados monitorados. Os resultados permitiram concluir que a utilização de ferramentas de monitoramento deixa a organização preparada para verificar o tráfego da rede e qual o melhor caminho a seguir com as informações que se tem. Assim, também se tem uma segurança extra, graças ao monitoramento, pois o mesmo faz uma varredura e verifica o que está sendo trafegado na rede e como está sendo esse tráfego. O Grafana desempenha um papel importante na melhoria do monitoramento de rede, permitindo aos administradores tomarem decisões, otimizar o desempenho e garantir a confiabilidade das operações da rede. Sua capacidade de visualização de dados, alertas em tempo real e integração com várias fontes de dados o tornam uma ferramenta valiosa para manter o funcionamento seguro das redes modernas.

Palavras-chave: Grafana, monitoramento de redes de computadores, redes de computadores, segurança de redes.

ABSTRACT

This work has the general objective of developing a study of the Grafana tool to describe its operation and show how its use facilitates the interpretation and understanding of monitored data. As the study is ongoing, the conclusion is partial. It was possible to conclude that the use of monitoring tools leaves the organization prepared to check network traffic and the best path forward with the information available. Thus, there is also extra security, thanks to monitoring, as it scans and checks what is being trafficked on the network and how this traffic is going. Grafana plays an important role in improving network monitoring, enabling administrators to make decisions, optimize performance, and ensure the reliability of network operations. Its data visualization capabilities, real-time alerts, and integration with multiple data sources make it a valuable tool for keeping modern networks running securely.

Key words: Grafana, computer network monitoring, computer networks, network security.

LISTA DE ILUSTRAÇÕES

Figura 1 – Rede LAN	16
Figura 2 – Rede WAN	17
Figura 3 - Análise de Link via SNMP	22
Figura 4 - Analisando servidor pelo Zabbix	23
Figura 5 - Analisando um servidor	24
Figura 6 – Análise de um banco de dados.	28
Figura 7 – Acessando o servidor para configuração	29
Figura 8 – Tempo de resposta de chamados	30
Figura 9 – Análise de Erros	31
Figura 10 – Configuração da CPU	35
Figura 11 – Utilização de CPU	36
Figura 12 – Configuração da Utilização da memória	36
Figura 13 – Utilização de memória	37
Figura 14 – Configuração de visualização do CPU e Memória	37
Figura 15 – Histórico de CPU e memória	38
Figura 16 – Quantidade de CPU’s	39
Figura 17 – Quantidade de CPU’s	39
Figura 18 – Configuração do Serviço de Ping	40
Figura 19 – Número de Ping	40
Figura 20 – Verificar o tráfego na rede	41
Figura 21 – Tempo ligado	41
Figura 22 – Número de processos rodando	42
Figura 23 – Quantidade de Processos	42
Figura 24 – Configuração de Disco	43
Figura 25– Discos utilizados	43
Figura 26– Configuração leitura e escrita do disco	44
Figura 27 – Histórico da utilização do disco	44
Figura 28 – Configuração de verificação do espaço no disco	45

Figura 29 – Espaço utilizado do servidor	46
Figura 30 – Verificar o tráfego na rede	47
Figura 31– Tráfego na rede	47
Figura 32 – Problema no Servidor	48
Figura 33 – Problemas no servidor	49
Figura 34 – Configuração de Switch	50
Figura 35 – Tráfego na porta do switch	50
Figura 36 – Portas do Switch	51

LISTA DE SIGLAS E ABREVIATURAS

API	*Content Delivery Network* ou Rede de Distribuição de Conteúdo
CD	*Continuous Delivery ou Entrega Contínua*
CDN	*Continuous Integration ou Integração Contínua*
CI	*Central Processing Unit ou Unidade Central de Processamento*
CPU	*Central Processing Unit ou Unidade Central de Processamento*
IP	*Internet Protocol ou Protocolo de Internet*
IPMI	*Intelligent Platform Management Interface ou Interface Inteligente de Gerenciamento de Plataforma*
JMX	*Java Management Extensions*
MS-DOS	*Microsoft Disk Operating System ou Sistema Operacional em Disco da Microsoft*
MYSQL	*My Structured Query Language ou Minha Linguagem de Consulta Estruturada*
NOSQL	*Not Only Structured Query Language ou Não Apenas Linguagem de Consulta Estruturada*
OMD	*Open Monitoring Distribution ou Distribuição de Monitoramento Aberto*
PING	*Packet Internet Network Grouper ou Agrupador de Pacotes da Internet*
RAM	*Random Acess Memory ou Memória de Acesso Aleatório*
RRDTOOL	*Round Robin Database Tool ou Ferramenta de Banco de Dados*
S	*Round Robin*
SNMP	*Simple Network Management Protocol ou Protocolo Simples de Gerenciamento de Rede*
SQL	Structured Query Language ou Linguagem de Consulta Estruturada

SSH Secure Socket Shell ou Shell de Soquete Seguro

TCP *Transmission Control Protocol ou Protocolo de Controle de Transmissão*

TI *Tecnologia da Informação*

TSDB *Time Series Database ou Banco de Dados de Séries Temporais*

VPN *Virtual Private Network ou Rede Virtual Privada*

SUMÁRIO

1 INTRODUÇÃO.....13
2 REFERENCIAL TEÓRICO.....16
2.1 Conceitos e definições.....16
2.1.1 REDES.....16
2.1.2 MONITORAMENTO.....17
2.1.3 As ameaças cibernéticas.....18
2.1.4 Importância da segurança de dados.....18
2.1.5 Principais ferramentas de monitoramento de redes.....19
2.2 Trabalhos relacionados.....22
2.2.1 Monitoramento de redes de computadores utilizando o protocolo SNMP.....22
2.2.2 Monitoramento de dispositivos em rede utilizando Zabbix e Grafana.....22
2.2.3 *Análise comparativa entre ferramentas para gerenciamento e monitoramento de redes*.....24
3 MÉTODO.....26
4 GRAFANA.....28
4.1 O que é o Grafana.....28
4.2 Instalação e configuração do Grafana.....32
5 APLICAÇÃO PRÁTICA DO GRAFANA.....35
5.1 CPU Utilizada.....35
5.2 Memória utilizada.....36
5.3 Histórico de CPU e memória.....37
5.4 Histórico de CPU e memória.....38
5.5 Total de CPU's.....38

5.6 ICMP ping.....40

5.7 Quanto tempo um servidor está ligado.....41

5.8 Quanto tempo um servidor está ligado.....41

5.9 Número de Processos sendo executados no Servidor.....41

5.10 Número de Processos sendo executados no Servidor.....42

5.11 Verificar a utilização de Discos.....42

5.12 Leitura e Gravação do Disco de um Servidor.....43

5.13 Leitura e Gravação do Disco de um Servidor.....44

5.14 Espaço Utilizado em Disco.....45

5.15 Espaço Utilizado em Disco.....45

5.16 Navegação.....46

5.17 Navegação.....47

5.18 Problemas no Servidor.....48

5.19 Problemas no Servidor.....48

5.20 Configuração de Switch.....49

5.21 Visualização do Tráfego.....50

5.22 Visualização do Tráfego.....51

6 CONCLUSÃO.....52

7 REFERÊNCIA.....53

1 INTRODUÇÃO

Desde o início dos anos 2010, a realidade sem a existência de redes é um contexto considerado impossível, e assim, com o passar dos anos, cada vez mais, as pessoas utilizam diversos serviços de rede, tais como as redes sociais, correios eletrônicos e mensagens instantâneas. Consequentemente, esses fatores são resultado do desenvolvimento tecnológico dos séculos anteriores (Macedo et al., 2018)

Segundo Tanenbaum (2021), uma rede de computadores são diversos computadores que funcionam de forma independente, porém conectados entre si, que realizam tarefas de uma determinada instituição, e que podem trocar informações, através da linguagem de protocolos.

Essas redes possuem diversos equipamentos que se desenvolvem com o avanço tecnológico, em níveis internos e externos, o que resulta na necessidade de constante suporte e monitoramento, para detecção de falhas presentes nos equipamentos (Carvalho,2020).

Sendo assim, o conceito de rede também surge da “camada de rede”, que é o encaminhamento de pacotes do seu ponto de origem até o seu destino, passando, assim por diversos dispositivos, tendo como finalidade, assim, de conduzir esses mesmos pacotes do remetente ao destinatário (Fernández, 2019).

Com o objetivo de planejar e aumentar a disponibilidade de seus recursos, surgiu a necessidade de monitoramento dessas redes. Contudo, esse processo é complexo para mãos humanas, sendo necessário a utilização de ferramentas automatizadas. (Júnior & Neves, 2019).

Consequentemente, o processo de monitoramento trata-se, de um gerente realizar o planejamento, instalação, operação e monitoramento de hardware e software, que fazem parte da rede de computadores. Com esse monitoramento, ocorre a possibilidade de correção de problemas detectados, que podem estar deixando a rede ineficiente (Hentges & Schorr, 2021).

Diante disso, o gerenciamento de redes é dividido em cinco categorias, sendo a de falhas, de desempenho, de configuração, de segurança e de contabilização (Hentges & Schorr, 2021). As principais funcionalidades do monitoramento são o bom funcionamento da rede, detectar e verificar o que foge

da normalidade, corrigindo assim o erro e possibilitando que a rede volte ao seu devido funcionamento (Belentani et al, 2018).

Justifica estudar este tema pois o Grafana é uma plataforma interativa de dados que permite os usuários monitorarem dados por tabelas e painéis interativos, com isso facilitando a compressão dos que está acontecendo na rede de computadores.

Diante deste contexto, este trabalho busca responder a seguinte questão de pesquisa – **"Como facilitar a interpretação de dados monitorados em uma rede de computadores visualizados por meio da ferramenta Grafana?"**

Este trabalho tem como objetivo geral desenvolver um estudo da ferramenta Grafana para descrever seu funcionamento e mostrar como seu uso facilita a interpretação e a compreensão dos dados monitorados na rede.

Os seus objetivos específicos são:

- Apresentar as funcionalidades da ferramenta Grafana;
- Mostrar a utilização da ferramenta para visualização dos dados monitorados na rede;
- Apresentar o funcionamento do Grafana em um ambiente real de monitoramento de redes;
- Listar o passo a passo da instalação do Grafana.

Espera-se que os resultados deste trabalho possam contribuir para:

- Informar aos administradores de redes de computadores sobre a instalação e a utilização desta nova ferramenta de visualização dos dados monitorados na rede de computadores;
- Mostrar o quanto a ferramenta Grafana pode facilitar na compreensão dos dados monitorados;

Considerando o aspecto metodológico, esta pesquisa é bibliográfica e experimental.

A monografia está organizada da seguinte forma: no capítulo 1, são apresentados o tema do trabalho, a questão de pesquisa, os objetivos e os resultados esperados. O capítulo 2 aborda o referencial teórico, incluindo conceitos, definições e trabalhos relacionados ao tema. O capítulo 3 fornece uma descrição do método, mostrando o passo a passo de como o trabalho foi conduzido e quais foram as ações realizadas para alcançar o objetivo geral. No

capítulo 4 é apresentado o funcionamento da ferramenta Grafana, como a ferramenta se comunica, os *Dashboards* para visualização do analista de redes, como seria a melhor prática para atender a rede da organização que está sendo utilizada. O capítulo 5 traz a utilização da ferramenta em um ambiente real e como seu funcionamento ajuda o analista de rede a verificar problemas na estrutura. Por fim, no capítulo 6 é apresentada a conclusão e sugestões de trabalhos futuros.

2 REFENCIAL TEÓRICO

2.1 Conceitos e definições

2.1.1 Redes

Redes são definidas como redes de computadores, muito utilizadas principalmente em ambientes organizacionais, pela quantidade de computadores, sendo que, que cada trabalhador utiliza um computador de forma individual. Com isso, os dados das máquinas da empresa são armazenados no servidor, que se situa em um local central, por um administrador de redes, conforme mostra a Figura 1 (Tanenbaum,2021).

Figura 1 – Rede LAN

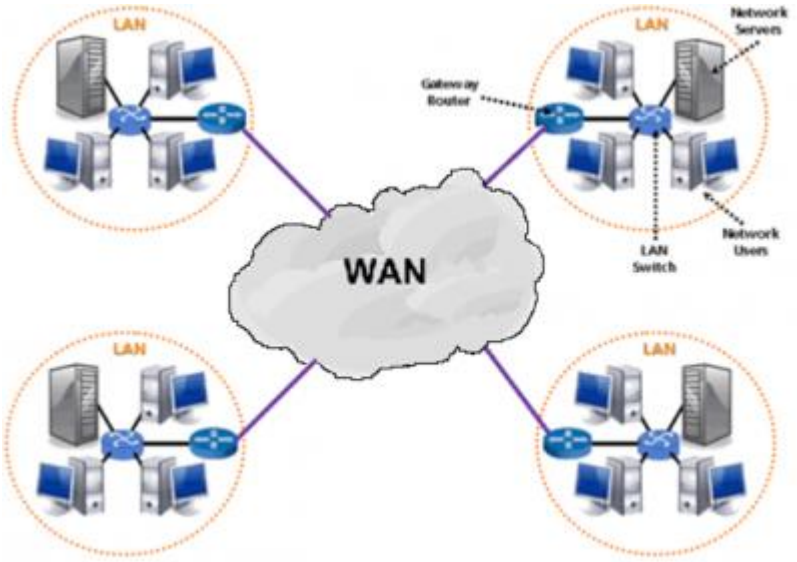
Fonte: REIS (2019)

Segundo Tanenbaum (2021), o objetivo da configuração de redes está ligado às pessoas, e não com as informações ou computadores. Nesse sentido, essas redes oferecem um importante meio de comunicação entre os sujeitos, possibilitando a troca de mensagens por correio eletrônico. Ligações telefônicas também podem ser realizadas pelas redes, através do IP.

Diante disso, o acesso de Internet da rede, em meio doméstico, permite conectividade entre computadores remotos e possibilita acesso à diversos conteúdos e sites diferentes, compra de produtos, além da comunicação e

interação de usuários, de forma virtual, conforme ilustra a Figura 2 (Tanenbaum, 2021).

Figura 2 – Rede WAN



Fonte: Reis (2019)

2.1.2 Monitoramento

A Internet é um local de inúmeras oportunidades inexploradas e, embora o campo de segurança de redes tenha avançado nos últimos anos, há redes de criminosos globais, capazes de invadir redes de informática. Contudo, a prática do Monitoramento de Segurança de Redes possibilita que ocorra a devida proteção dessas redes (Sanders & Smith, 2014).

Ainda segundo Sanders & Smith (2014), Monitoramento de Segurança de Redes, é a coleta e detecção de dados de segurança de uma rede. Além disso, a segurança de informação é dividida em diversas áreas, com focos distintos, como proteção, concentrada na segurança de sistemas, evitando a invasão da mesma.

Sucessivamente, também há a área de detecção, com o objetivo de detectar os comprometimentos que estão ativos ou que já estavam ativos anteriormente. Esta tarefa incluí o monitoramento de segurança, além de ataques à rede. Em seguida, há o domínio de resposta, que se concentra na resposta, após uma meta ter sido alcançada, que envolve a redução de

incidentes, análise de rede, *host malware* e relatório de incidentes (Sanders & Smith, 2014).

Os autores Sander & Smith (2014) também afirmam sobre o domínio de sustentação, que é a fase final, que trata o gerenciamento de pessoas, processos e tecnologia *Content Delivery Network* (CDN), que incluí treinamento, desenvolvimento e implementação de tecnologia e sistemas de suporte e de gerenciamento.

2.1.3 As ameaças cibernéticas

As ameaças cibernéticas são formas de grupos de sujeitos, ou de apenas ação de sujeito individual, de modificar, expor, roubar informações pertencentes às organizações ou outras pessoas. Assim, há diversas formas de invasões, como *Denial of Service* (DoS), utilizado com o objetivo de bloquear a entrega dos serviços pertencentes ao fornecedor. Diante disso, ele realiza a requisição de um dispositivo, resultando na sobrecarga de processamento, banda, memória e a *Central Processing Unit* (CPU) do computador (Bonguet, 2017; Teixeira, 2021).

Segundo Fornasier *et al* (2020), outra forma de ataque são os *malwares*, de caráter malicioso, sendo que o mais conhecido é o ataque *Ransonware,* sendo que sua principal função é a extração de informações, que são criptografadas. Em seguida, é solicitado um resgate, para que o usuário tenha acesso aos dados. Sendo assim, essa ação é considerada um sequestro digital, que rouba dados que podem ser vitais e essenciais de organizações.

Além de extorsão os dados, os criminosos virtuais também vendem essas informações para os provedores, para que não precisem negociar com terceiros, que consequentemente poderiam dificultar a negociação, podendo expor o esquema de roubo (Fornasier *et al*, 2020).

2.1.4 Importância da segurança de dados

É importante o asseguramento da proteção e sigilo de dados, de natureza pessoal ou organizacional, além de movimentações bancárias e de senhas. Sendo assim, é necessário a proteção de acessos não autorizados, de

dados confidenciai, além dos danos acidentados ou intencionais, ademais, também a execução de políticas e processos para a recuperação das violações e perdas de informações (Teixeira et al, 2021).

Em relação à proteção de informações, a criptografia é considerada a mais eficaz, impedindo que indivíduos que não possuem autorização acessem mensagens, através da criação e avaliação de protocolos de segurança. Além disso, a *Virtual Private Network* (VPN) também é uma ferramenta com extrema importância para a segurança cibernética de organizações, que interliga duas ou mais computadores, em uma conexão privada e segura (Teixeira *et al*, 2021).

Além disso, a segurança cibernética são ações voltadas para a segurança da informação, que propõe prevenir ataques cibernéticos, que aproveitam de falhas no sistema, para explorar diversos dispositivos, com o intuito de extorquir dados e arquivos, tornando-os indisponíveis (Schultz, 2020).

2.1.5 Principais ferramentas de monitoramento de redes.

Zabbix é um software de gerenciamento de host, (lançado em 2001), que possuí como principal característica a análise remota de serviços, criação de alertas, além da criação de relatórios após o processo de avaliação, podendo também realizar, através da obtenção e transformação de dados coletados, a criação de gráficos e estatísticas do servidor. Além disso, o programa possibilita uma maior flexibilidade na efetuação da coleta de dados, além da realização de processamento de forma mais complexa (Arcenio, 2015; Bueno & Weingarter, 2022).

Segundo Leandro (2019), a função primordial do Zabbix reside na sua capacidade de efetuar o monitoramento e análise de dados. Os ganhos inerentes a uma análise de dados eficaz, os quais incluem identificação e a prevenção de problemas. Assim, relativo aos dados que são coletados pelo sistema Zabbix, este oferece a capacidade de armazená-los, possibilitando sua posterior utilização e permite uma organização flexível de acordo com as necessidades individuais de cada utilizador.

No que tange à segurança, a plataforma Zabbix adota um sistema de criptografia e autenticação, visando garantir um nível elevado de proteção. Outra vantagem altamente valorizada é a facilidade de criação e manipulação de

objetos e dados. No contexto das configurações, é relevante observar que a instalação do Zabbix é relativamente simples e rápida, sendo compatível com os principais sistemas operacionais e plataformas. Quanto à sua gestão, a plataforma dispõe de uma interface web intuitiva e customizável, adaptando-se aos perfis individuais de cada cliente. Adicionalmente, o Zabbix destaca-se pelo seu compromisso com o código aberto, evitando qualquer forma de dependência de fornecedor (Leandro, 2019).

O Nagios, lançado em 1996, se destaca por ser uma ferramenta de monitoramento de código aberto, que apresenta como função a checagem dos status dos equipamentos de rede, através de um *Packet Internet Network Grouper* (Ping) em um *Microsoft Disk Operating System* (MS-DOS). Diante disso, o *Nagios* apresenta como principais vantagens o seu design prático e simples, possibilitando também a redução de custos, por parte das empresas que o utilizam, além de trazer uma visão mais complexa da situação da empresa (Fornaroli & Alves, 2021).

O *Cacti,* lançado em 2001, é uma ferramenta que visa o auxílio nas tarefas de monitoramento de rede, sendo uma aplicação *open source*, que realiza o recolhimento e exibição de informações sobre o atual estado da rede de computadores. Além disso, o software possuí como vantagens a facilitação da visualização de informações de largura de banda, espaço do disco e uso da CPU, através de gráficos (Silva & Souza, 2019).

As informações abaixo foram retiradas do site *Networking* (2023). Segundo ele, a ferramenta *Paessler Network Monitor (PRTG),* lançado em 2003, é utilizada para monitorar dispositivos de rede, além de seu tráfego, desempenho e suas aplicações. Assim, seu ponto forte é a usabilidade, possibilitando um monitoramento em movimento e possibilitando varredura de rede e acionamento automático de elementos de monitoramento.

Ademais, esse software possibilita o alerta em tempo real, personalizável, tornando a resolução de problemas mais facilitada. Além disso, pode-se utilizar a definição de limites individuais e gatilhos de notificação, resultando na redução do chamado *alert noise*.

Em 2023, também há diversas outras opções de softwares de monitoramento, como o *LogicMonitor, lançada em 2008,* caracterizado como uma ferramenta na função nuvem, utilizada para o monitoramento a saúde o

desempenho dos dispositivos de tráfego da máquina. Em relação à sua opção de visualização, o software pode ser considerado limitado, porém pode favorecer mapas interativos, que podem consequentemente chegar à raiz de um problema, encontrado na rede durante o monitoramento.

Existe também a ferramenta *Checkmk, lançada em 2007, caracterizada* como um software abrangente de monitoramento de aplicativos. Sendo assim, ela utiliza o escaneamento de rede, em busca de dispositivos e também serviços, iniciando assim uma configuração automática e iniciando um monitoramento. Ainda sobre a *Checkmk*, ela oferece um alto número de verificações que já estão pré-configuradas, para todos os tipos de fornecedores e provedores de rede, podendo, assim, auxiliar no monitoramento de diversos componentes. Porém, muitos destes *plug-ins* possuem como base agentes, e necessitam de configurações mais complexas.

Ademais, o ponto forte do software pode ser considerado do conceito de configuração baseado em regras. Diante disso, pode-se configurar regras de monitoramento especificas, que podem ser aplicadas e implementadas em todos os dispositivos envolvidos de rede.

Por fim, existe *Datadog, lançado em 2010*, uma plataforma de monitoramento sintética e real, que possibilita o gerenciamento de log, além do desempenho de diversos aplicativos. Diante disso, o software é baseado em nuvem, que possuí funções de monitoramento de rede, insights sobre a saúde e desempenho do dispositivo, bem como seus tráfegos de rede e outros aspectos de sua infraestrutura. Uma vantagem desta ferramenta é a sua capacidade de visualizar dados de monitoramento, com painéis e mapas atraentes, no sentido visual, além da opção de personalização dos mesmos, através de recursos do tipo “arrastar” e “soltar”, sendo possível a partir de uma gama de widgets de visualização.

2.2 Trabalhos relacionados

Esta seção apresenta alguns trabalhos relacionados ao tema em estudo.

2.2.1 *Monitoramento de redes de computadores utilizando o protocolo SNMP.*

Hentges & Schorr (2021), utilizaram a ferramenta de monitoramento, *Simple Network Management Protocol (*SNMP), que é considerado o protocolo padrão mais simples, utilizado por diversos fabricantes e operadores. Essa ferramenta troca seus protocolos com uma entidade de gerenciamento e também um agente, e assim, diante disso, o gerente coleta dados e administra suas ações dos agentes, de forma conjunta, gerando assim relatórios de execução de atividades mais difíceis, conforme mostrado na Figura 3.

Figura 3 – Análise de Link via SNMP

Fonte: Autoria própria

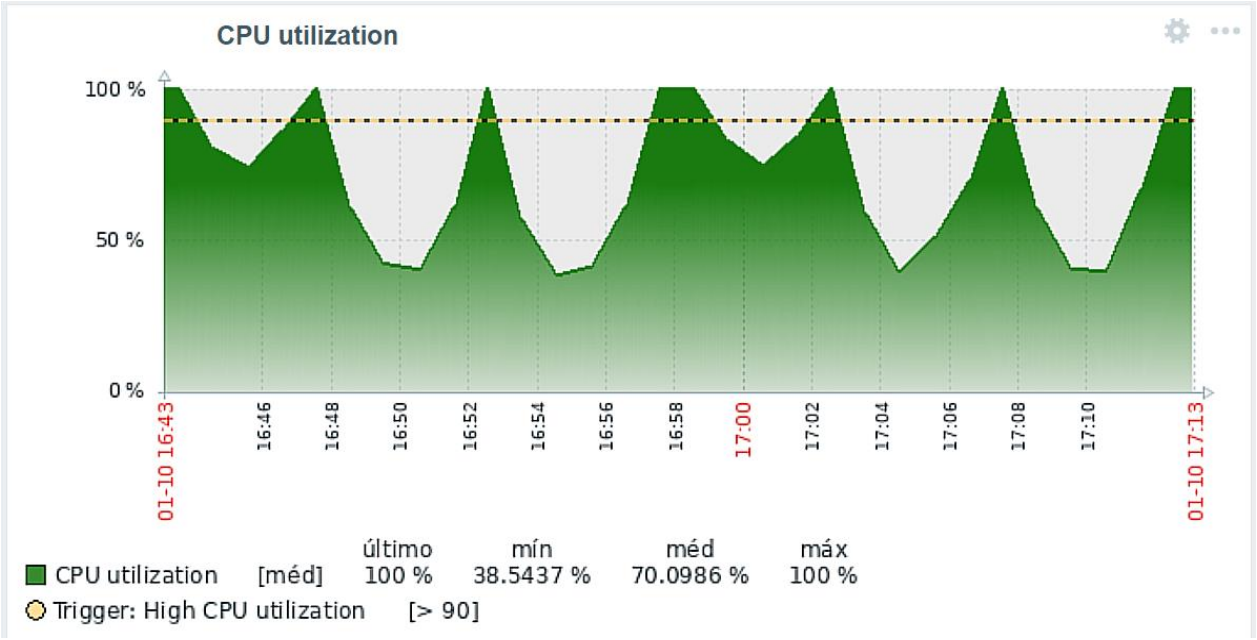
2.2.2 *Monitoramento de dispositivos em rede utilizando Zabbix e Grafana.*

Bueno & Weingarter utilizaram o *Zabbix*, uma ferramenta, que realiza o gerenciamento de host, e assim como o *Grafana*, também realiza o armazenamento de informações presentes no banco de dados. Além disso, a

ferramenta possibilita a monitoração de vários parâmetros, como desempenho, performance e integridade do servidor de rede.

O *Zabbix* também analisa serviços de forma remota, e assim, o sistema alerta os agentes sobre os itens que estão sendo avaliados, para que o servidor possa criar relatórios sobre os sistemas que foram avaliados, além de também processa dados em gráficos e estatísticas, conforme ilustrado na Figura 4 analisando o servidor pelo *Zabbix.*

Figura 4 – Analisando servidor pelo Zabbix



Fonte: Autoria própria

Já o Grafana foi utilizado pelos autores para uma melhor visualização dos resultados, pois o software possuí painéis mais detalhados sobre os dados avaliados, conforme mostrado na Figura 5.

Figura 5 – Analisando um servidor

Fonte: Autoria própria

Nota-se na Figura 5 que está sendo usado 36% de memória, 7% de CPU e 697 processos em utilização. Dessa forma o Grafana mostra visualmente e facilita o monitoramento da rede de computadores.

2.2.3 Análise comparativa entre ferramentas para gerenciamento e monitoramento de redes.

Andreoli (2016) realiza um comparativo entre três softwares de monitoramento, sendo eles o *Open Monitoring Distribution* (OMD), *Cacti* e *Zabbix,* visando determinar qual deles se comporta no ambiente de ensaio escolhido pelo autor. Diante disso, o cenário utilizado para o ensaio foi a cidade de São Lourenço, localizada em Santa Catarina.

Em relação a ferramenta OMD, ela é caracterizada de monitoramento de *open source,* tendo como principal objetivo a facilitação da configuração do Nagios, na qual o software foi baseado, além de possibilitar a disponibilização de diversos *plug-ins*, para que ocorra a melhora e a facilitação do processo de

gerenciamento. Ademais, a Cacti é uma ferramenta desenvolvida pela *Round Robin Database Tool (RRDTool)* com o intuito da criação de gráficos e armazenamento de dados da rede em uma base de dados, a M*y Structured Query Language* (*MySQL) (*Andreoli, 2016).

Além desses softwares, foi usado o *Zabbix,* que monitora a disponibilidade, qualidade de serviço da ferramenta e também a experiência do usuário. Por fim, no comparativo, Andreoli (2016) concluiu que a ferramenta Zabbix esteve em 1º lugar em 9 das 14 métricas avaliadas Versatilidade, Monitoramento em Tempo Real, Flexibilidade e Customização, Escalabilidade, Alertas e Notificações, Interface Intuitiva, Relatórios, Gráficos Open Source e Requisitos de Hardware, seguido do software *OMD*. Ademais, em última colocação se manteve o *Cacti. D*iante disso, chegou-se à conclusão de que o Zabbix apresentou melhor índice geral na análise realizada (Andreoli, 2016).

3 MÉTODO

Essa pesquisa, segundo sua natureza, é um resumo de assunto, que tem como objetivo realizar a sistematização de uma área de conhecimento, realizando, assim, sua evolução histórica e estado de arte (Wazlawick, 2014, p.21).

Quanto aos objetivos, é uma pesquisa exploratória e descritiva. Diante disso, segundo Gil (2017), a pesquisa exploratória tem como objetivo elaborar uma maior familiaridade com determinado tema, com planejamento flexível, que elabora novas ideias sobre o assunto, tornando-o mais compreensível e podendo também elaborar hipóteses.

Já a pesquisa descritiva tem como principal objetivo a descrição de características de um determinado fenômeno, além de estabelecer relações entre suas variáveis, e utiliza técnicas padrões de coleta de informações, como questionários e observação sistemática (Gil, 2017, p.42).

Segundo seus procedimentos técnicos, esta pesquisa é classificada como bibliográfica e documental.

A pesquisa bibliográfica envolve o estudo de artigos, teses, livros e outras publicações disponibilizadas por editoras e indexadas. É um passo essencial e preliminar para qualquer trabalho científico, porém, por si só, não gera novo conhecimento. Assim, possuí como principal propósito fornecer ao pesquisador informações públicas que ele ainda não possuía, disponibilizando ao pesquisador informações e referências relevantes para apoiar sua pesquisa (Wazlawick, 2014, p.23).

Segundo Gil (2017) essa pesquisa responde as seguintes questões:

a) Escolha do tema: Monitoramento de redes de computadores utilizando Grafana.

b) Levantamento bibliográfico preliminar: Realizar o levantamento bibliográfico auxilia o pesquisador a se familiarizar com a área de estudo escolhida, o que facilita a identificação e definição do problema.

c) Formulação do problema: - Como facilitar a interpretação de dados monitorados em uma rede de computadores visualizados por meio da ferramenta Grafana?

d) Busca das fontes: Foram realizadas consultas em dissertações, periódicos científicos, obras de referência e outros.

e) Leitura do material: adquirir informações com os materiais lidos e relacionar com o objetivo da pesquisa.

f) Fichamento: foi realizado fichamento de todos os materiais interessantes que contribuíam para o objetivo de pesquisa.

g) Redação do texto: escrita do TCC.

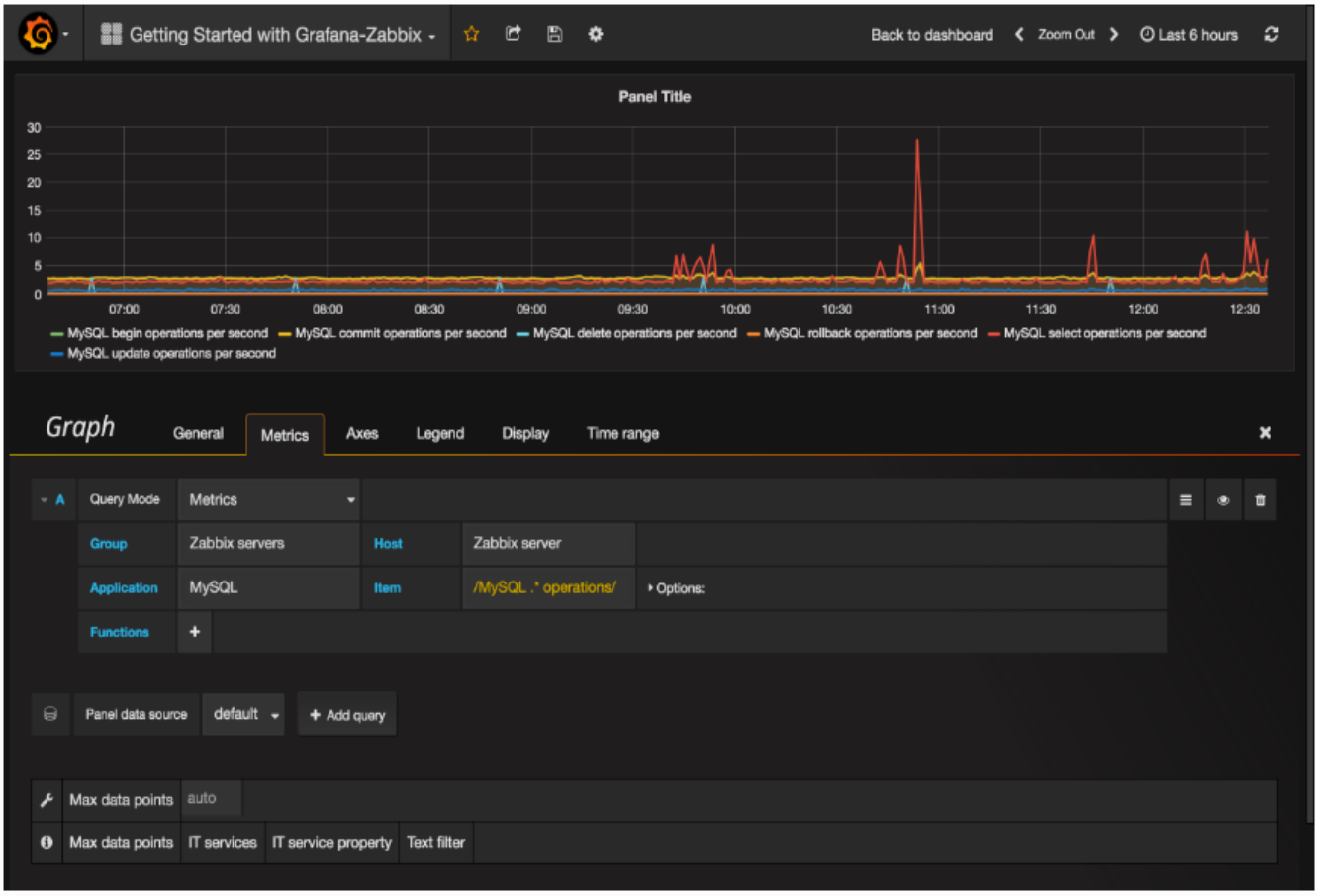
4 O GRAFANA

4.1 O que é o Grafana

Este capítulo tem como referência principal o site Grafana Labs (Grafana, 2023), que documenta a ferramenta Grafana.

O software Grafana, lançado em 2014, é um código aberto, que permite a consulta, visualizar, alertar, e explorar suas métricas, logs e rastreamentos, onde quer que os mesmos estejam armazenados. Diante desse contexto, o Grafana fornece ferramentas para a transformação de informações do banco de dados, de *Times Series Datebase* (TSDB), em gráficos e visualizações, conforme mostrado na Figura 6.

Figura 6 – Análise de um banco de dados.

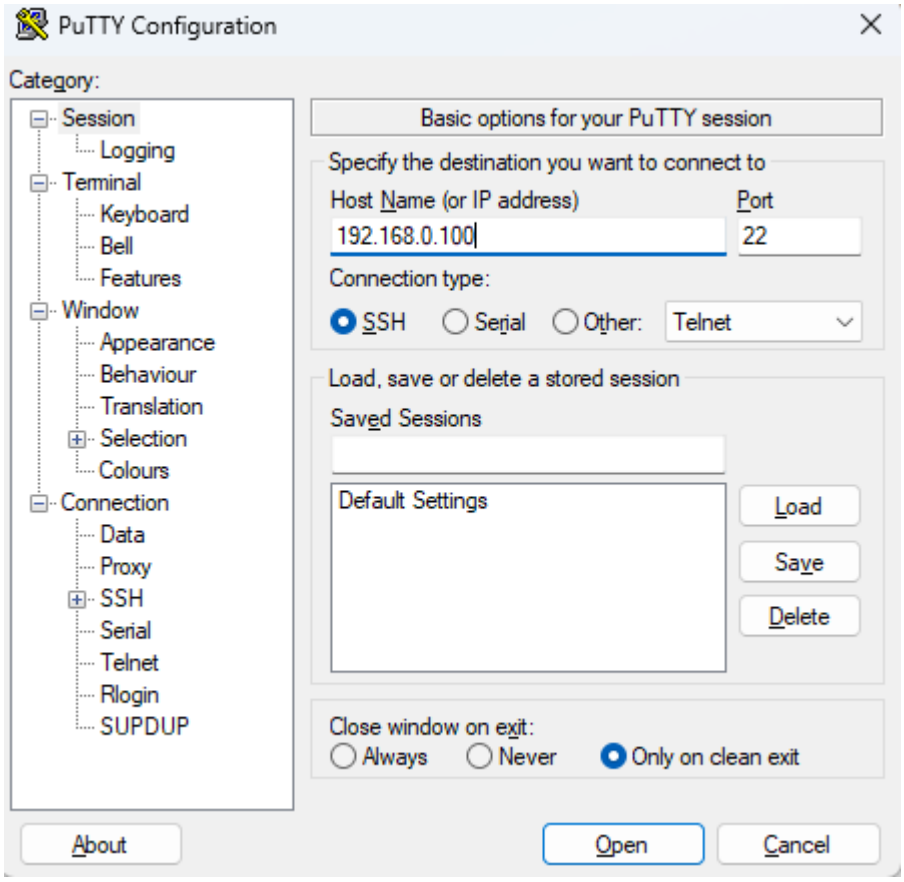


Fonte: Grafana (2020).

A estrutura do *plug-in* deste software oferece a flexibilidade de se conectar a diversas fontes de dados, incluindo bancos de dados *NoSQL* e *SQL*, como *Jira* ou *ServiceNow*, além de ferramentas de *Continuous Integration* (CI) e *Continuous Delivery* (CD), como *GitLab*. O Grafana é capaz de se integrar com uma ampla variedade de fontes de dados, que geralmente incluem bancos de dados como *Graphite, Prometheus, Influx DB, ElasticSearch, MySQL*, PostgreSQL e outros. Após a instalação, o Grafana permite que administradores de empresas gerenciem o software para várias equipes, possibilitando a configuração do provisionamento e autenticação de redes.

O Grafana é um software relativamente fácil de configurar, todavia, para ser instalado, é necessário cumprir alguns requisitos para ser executado. Diante disso, é preciso ter familiaridade com o *Powershell* para Windows, já para terminais Linux o *Secure Socket Shell* (SSH) será usado (Salituro, 2020), conforme mostra a Figura 7.

Figura 7 – Acessando o servidor para configuração



Fonte: Autoria própria

Segundo o site Profissionais da TI (2018), a comunidade do Grafana é considerada participativa e interativa, sendo que seus desenvolvedores documentam diversas informações nos fóruns, resultando em uma maior facilidade para a resolução de problemas relacionados ao mesmo. Outras funções da ferramenta é a criação de chamados, além de gráficos de chamados abertos mensalmente, além de possibilitar a junção de indicadores de diversas fontes.

Além disso, o gerente de suporte pode ter reunido no *dashboard* que demonstra as principais métricas do atendimento, via telefone, chat e ferramentas de chamados e monitoramento, todos reunidos no mesmo painel, facilitando a visão monitorada pelo gerente, segundo ilustra a Figura 8 (Profissionais da TI, 2018).

Figura 8 – Tempo de resposta de chamados

Fonte: Pacheco, 2017

Entre essas métricas, o site (Gocache, 2021) indica que há o *Grafana Cloud*, que consiste em uma plataforma de métricas de software aberta bem gerenciada e disponível, e assim, essa ferramenta é útil para programadores que não tem o objetivo de realizar a hospedagem de soluções localmente, e que não desejam se preocupar com o gerenciamento total da infraestrutura.

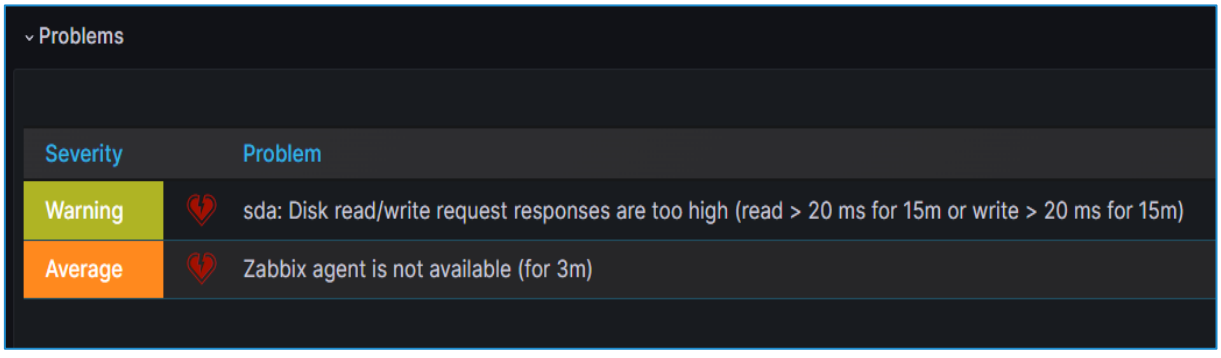
Sucessivamente, há a ferramenta *Grafana Enterprise,* que possui todos os recursos do *Grafana Cloud*, com *plug-in premiuns,* além de fontes de dados e suporte premium para a equipe principal que se encarrega do monitoramento. Ademais, também há *Phometheus Grafana*, uma ferramenta de monitoramento aberta. Assim, o painel do Grafana é utilizado para a visualização de dados, e as consultas são retiradas do painel, e os dados são adquiridos pelo Phometheus (Gocache, 2021).

Segundo o site GrafanaLabs (2023), *o Grafana Open Source* é um software de visualização e avaliação de código aberto. Assim, ele permite a consulta, visualização, alerta e exploração as suas métricas, logs e rastreamentos, de elas estejam armazenadas. Ademais, esse software fornece ferramentas para a transformação de informações do banco de dados do TSDB, em gráficos dinâmicos.

Outra ferramenta é o software *Grafana Loki*, sendo caracterizado como um conjunto de componentes de códigos abertos, compostos em *logs* com todos os recursos. Do mesmo modo, pode-se citar o *Grafana Tempo*, um back-end de rastreamento, que é distribuído de código aberto, de uso facilitado.

Já o *Grafana Mimir* é um projeto de software que fornece o armazenamento escalonável de longo prazo, para o *Prometheus*, em seguida, há o *Grafana Oncall*, caracterizado como ferramenta de gerenciamento de resposta a incidentes de código aberto. Diante disso, essa ferramenta foi produzida para auxiliar equipes a otimizar sua colaboração para a resolução de problemas, com mais rapidez, exemplo de um problema, segundo mostrado na Figura 9.

Figura 9 – Análise de Erros



Fonte: Autoria própria

Por fim, sua versão atual é o Grafana 10.1, sendo que suas principais atualizações foram a melhoria nos gráficos, com a adição de quatro novos recursos, como a Visualização Sanduíche, Alternância do esquema de cores, Alternância do alinhamento do nome do símbolo e, por fim, a Navegação aprimorada (Grafana, 2023).

Diante das informações apresentadas anteriormente, a Visualização Sanduíche mostra para o usuário todos os chamados, na parte superior, e todos os destinatários, na parte inferior. Essa ferramenta se torna útil para a visualização do contexto de um símbolo. Em seguida, a Alternância de cores possibilita que o programador alterne o esquema de cores em gradiente, com base no valor relativo do símbolo, ou no pacote de símbolo.

Já a Alternância de alinhamento do nome do símbolo permite alinhar o texto à esquerda ou à direita, possibilitando melhor diferenciação do nome de cada símbolo. E por fim, a Navegação aprimorada tem como objetivo destacar um símbolo ou ativar a visualização em sanduíche, para um símbolo de tabela, além de possibilitar uma barra de status, na parte superior do gráfico, que exibe visualizações que estão habilitadas no momento.

4.2 Instalação e configuração do Grafana

Segundo o site oficial do Grafana (2023), utiliza-se uma máquina virtualizada para criação do servidor e comunicação do Grafana com o Zabbix. Assim, a máquina era um sistema Linux Ubuntu Server 22.04, com 2 *gigabytes* de memória *Random Acess Memory* (*RAM)* e 1 processador lógico.

Em seguida, para fazer a atualização do sistema operacional com o comando: *apt-get update* após fazer a atualização foi instalado o Grafana com o repositório no *GitHub* usando o comando:

1) Instalação do pacote de pre-configuração

sudo apt-get install -y apt-transport-https software-properties-common wget
Comando *sudo:* executa tarefas que exigem permissões root ou administrativas*;*

O apt-get é uma ferramenta de linha de comando para lidar com as bibliotecas da *Advanced Package Tool* (APT) no Linux.
A linha de comando do Linux permite que seja baixado arquivos da Internet usando o comando wget. (Ariane G. 2023)

2) Importação da chave de configuração:

sudo mkdir -p /etc/apt/keyrings/
mkdir: cria um novo diretório.

wget -q -O - https://apt.grafana.com/gpg.key | gpg --dearmor | sudo tee /etc/apt/keyrings/grafana.gpg > /dev/null

3) Adicionando um repositório da versão mais estável, executando o seguinte comando:

echo "deb [signed-by=/etc/apt/keyrings/grafana.gpg] https://apt.grafana.com stable main" | sudo tee -a /etc/apt/sources.list.d/grafana.list
Comando echo = O comando echo é um utilitário nativo que exibe uma linha de texto ou cadeia de caracteres (string) usando a saída padrão. (Ariane G. 2023)

4) Atualiza-se novamente o sistema com o comando:
sudo apt-get update

5) Utiliza-se a ferramenta Enterprise, com isso usa-se o comando:
sudo apt-get install grafana-enterprise

6) Agora, inicia-se o Servidor Grafana no sistema com os comandos abaixo:
Para iniciar o serviço:

sudo systemctl daemon-reload
sudo systemctl start grafana-server
sudo systemctl status grafana-server

Systemctl para gerenciar serviços e unidades do como reiniciar serviços, ligar, desligar ou verificar os status da aplicação. ()

7) Verifica-se se o serviço está sendo executado:

   sudo systemctl status grafana-server

8) Configura-se o servidor do Grafana:

   sudo systemctl enable grafana-server.service

9) Reinicia-se o serviço do servidor para subir:

   sudo systemctl restart grafana-server

10) Para iniciar o servidor é necessário usar os comandos onde o *start* é para iniciar e o *status* e verificar se está correto. (Justin Ellingwood, 2020)

    sudo service grafana-server start
    sudo service grafana-server status

11) Abra o navegador e acesse o site http://localhost:3000/ para acessar o Grafana a porta 3000 é o padrão.
    Assim, está instalada a ferramenta Grafana.

5 Aplicação prática do Grafana

Nesse capítulo será mostrada a aplicação da visualização do monitoramento da rede pela ferramenta Grafana em um ambiente real.

A empresa será chamada de X para manter a sua privacidade. Ela é uma instituição financeira que está sendo monitorada pela ferramenta Zabbix 6.4.9, possuindo aproximadamente 1300 máquinas, incluindo servidores, desktops, switch, firewalls e nobreaks. A ferramenta Grafana está integrada com os softwares Zabbix e PTRG, para juntos realizarem o monitoramento e a visualização dos dados monitorados.

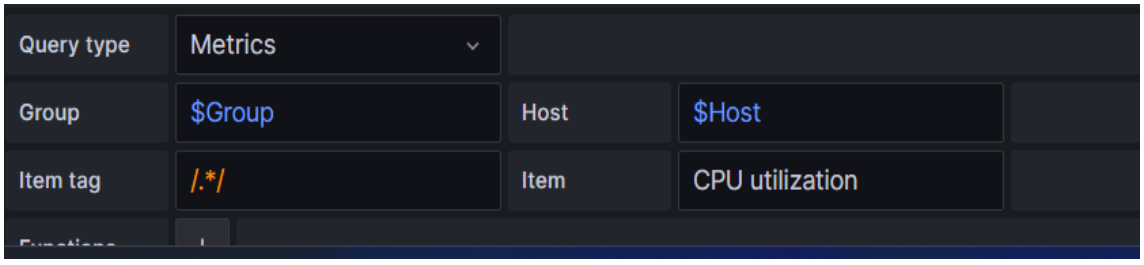
O Grafana visualiza os links de Internet com a comunicação via SNMP, juntamente com os firewalls para verificar o tráfego em tempo real.

Os testes realizados comprovaram que as visualizações mostradas pela ferramenta Grafana realmente facilita a compreensão e agiliza o monitoramento da rede.

5.1 CPU Utilizada

Para acompanhar o desempenho da CPU, o Grafana, integrado ao Zabbix através de um agente, obtém dados do servidor do host especificado. No Grafana, é solicitado qual métrica de utilização da CPU para o host está sendo usada, como ilustrado na Figura 10. A Figura 10 mostra como se faz a configuração para o host.

Figura 10 - Configuração da CPU



Fonte: Autoria própria

A Figura 11 exibe o uso atual da CPU como sendo de 8,72%, evidenciando a eficiência do monitoramento em tempo real do desempenho do servidor através da integração do Grafana com o Zabbix.

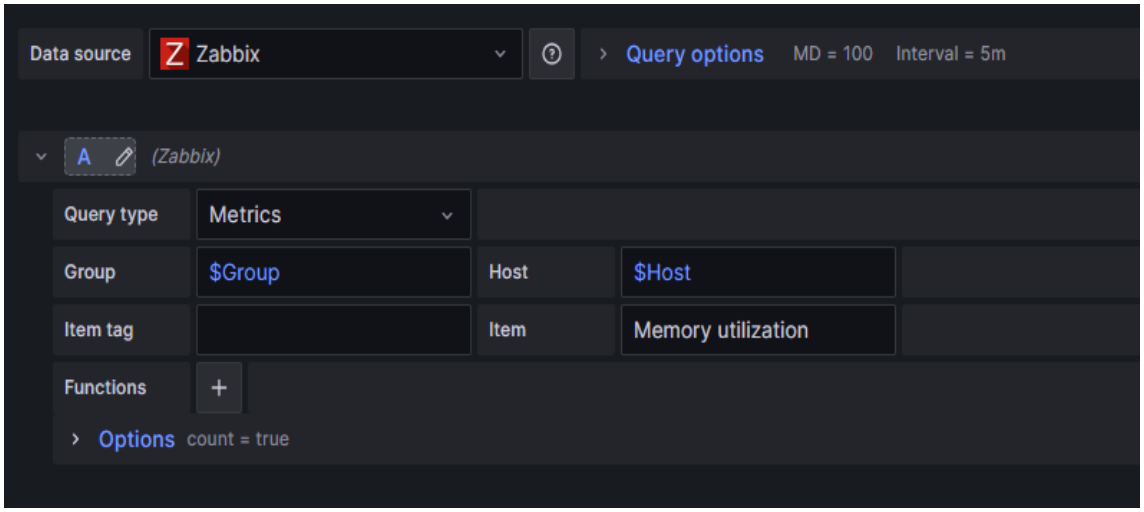
Figura 11 - Utilização de CPU

Fonte: Autoria própria

5.2 Memória utilizada

Para monitorar o uso de memória, o Grafana, que está conectado ao Zabbix por meio de um agente no servidor do host, está configurado para solicitar informações sobre a utilização da memória do host, como representado na Figura 12.

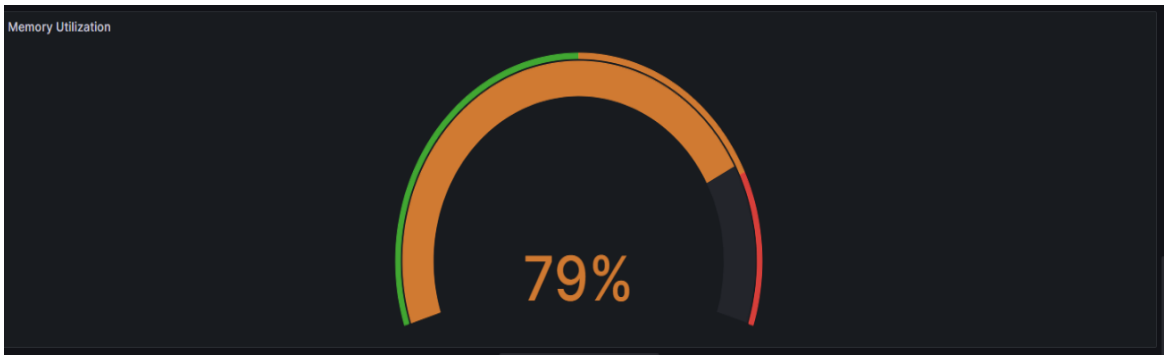
Figura 12 - Configuração da Utilização da memória



Fonte: Autoria própria

Após a configuração da utilização da memória, o resultado é exibido na forma do gráfico da Figura 13, indicando a porcentagem de uso. A Figura 13 indica que 79% da memória RAM do servidor está sendo utilizada.

Figura 13 - Utilização de memória

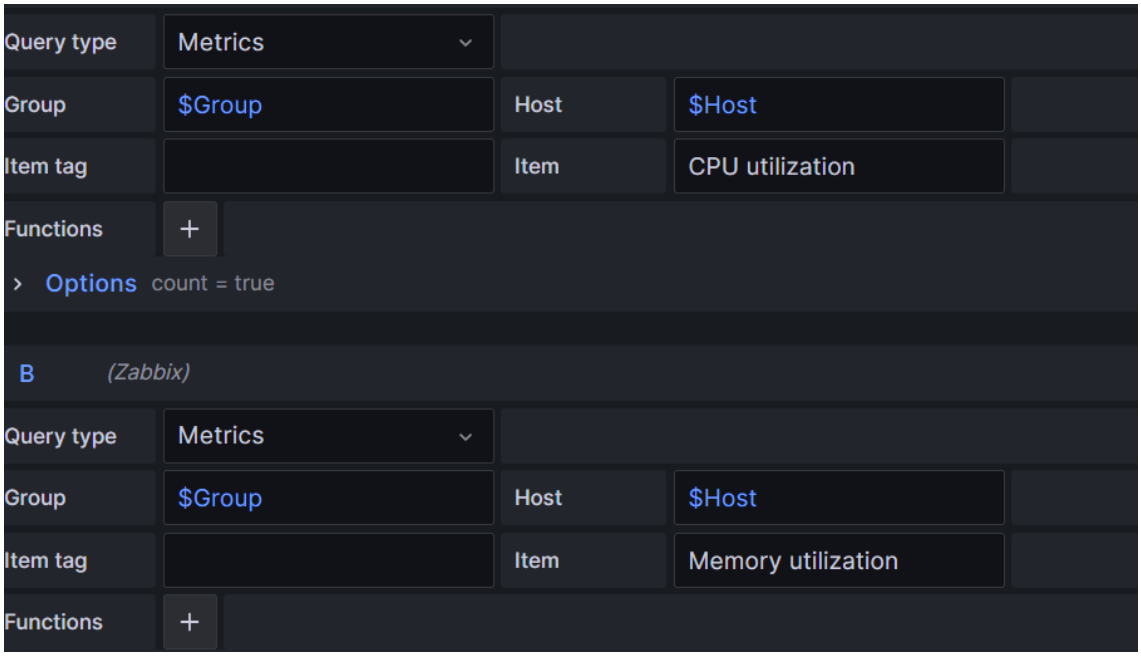


Fonte: Autoria própria

5.3 Histórico de CPU e memória

A configuração na Figura 14 mostra como e feito para visualizar a CPU e memória utilizando o Grafana. A consulta é feita com a de coletar métricas do serviço *Cpu utilization* e *memory utilization*. As variáveis Group e Host são utilizadas para permitir a seleção dinâmica de grupos e hosts dentro do Zabbix, permitindo uma verificação detalhada e específica do uso da leitura e escrita nos servidores monitorados.

Figura 14 – Configuração de visualização do CPU e Memória

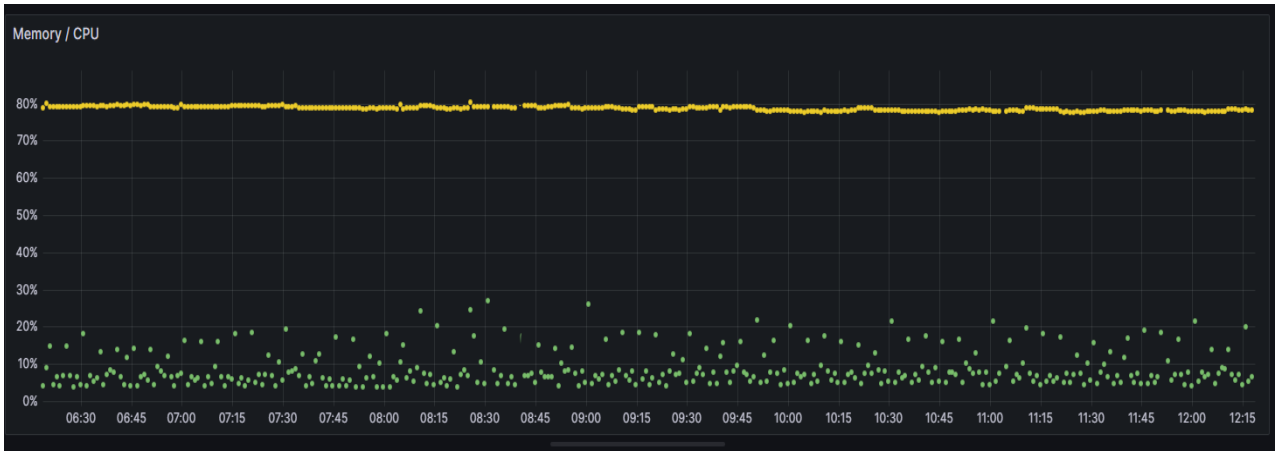


Fonte: Autoria própria

5.4 Histórico de CPU e memória

A Figura 15 mostra o acompanhamento do uso da memória RAM e da CPU ao longo de 5 horas, (das 6:30 da manhã até 12:30). A linha amarela, representa o uso da memória. No caso, se mantém estável, enquanto o gráfico verde, representa a CPU. No caso, ilustra a variação no uso da CPU ao longo do tempo, com os picos de utilização claramente visíveis.

Figura 15 – Histórico de CPU e memória

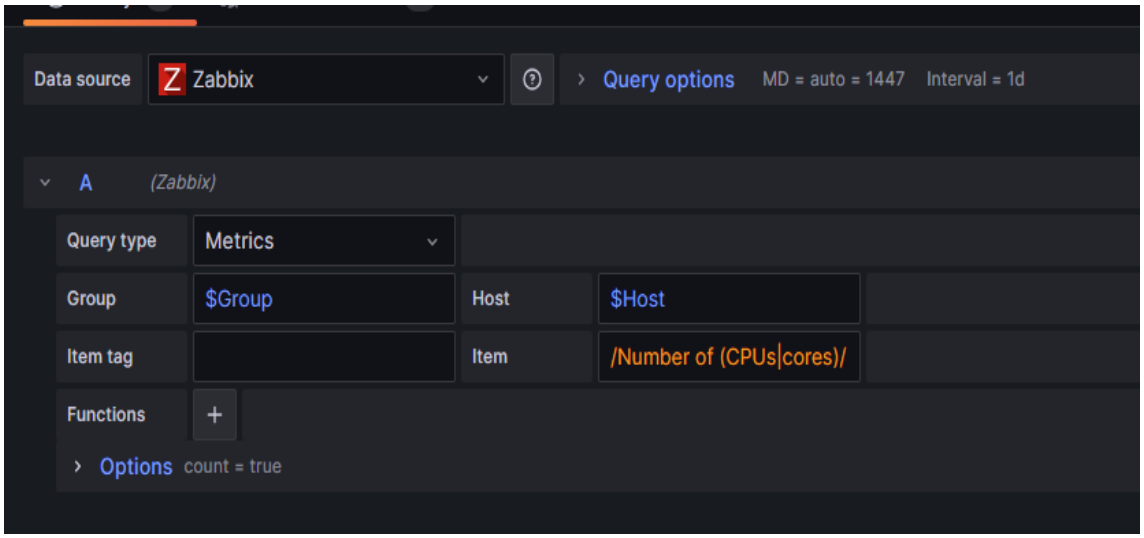


Fonte: Autoria própria

5.5 Total de CPU’s

A Figura 16 ilustra a configuração realizada para verificar o número de virtual CPUs em uso no servidor. Utilizando o Grafana com fonte de dados Zabbix, a consulta é configurada para extrair métricas específicas, neste caso, o total de CPUs virtuais ativas no host selecionado.

Figura 16 – Quantidade de CPU’s



Fonte: Autoria própria

A Figura 17 exibe o total de CPUs/cores presentes no servidor, que, conforme indicado, é de 4.

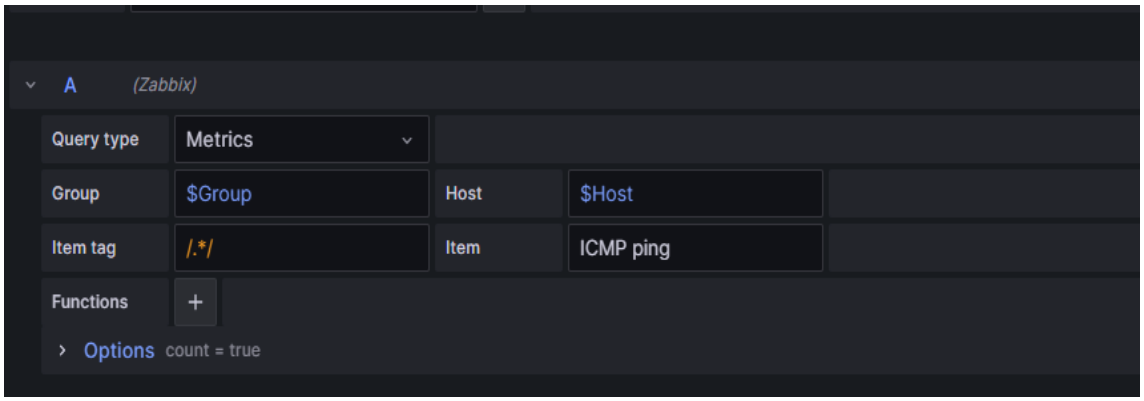
Figura 17 – Quantidade de CPU’s

Fonte: Autoria própria

5.6 ICMP ping

A Figura 18 mostra como configurar o Grafana com a fonte de dados Zabbix para verificar a disponibilidade e a latência de um servidor através do ICMP *ping*. A configuração inclui a seleção do tipo de consulta como *'Metrics'*, a especificação do grupo e do host e a definição do item de monitoramento como 'ICMP *ping'*. As opções adicionais permitem refinar a consulta para obter contagens precisas ou outros dados agregados conforme necessário.

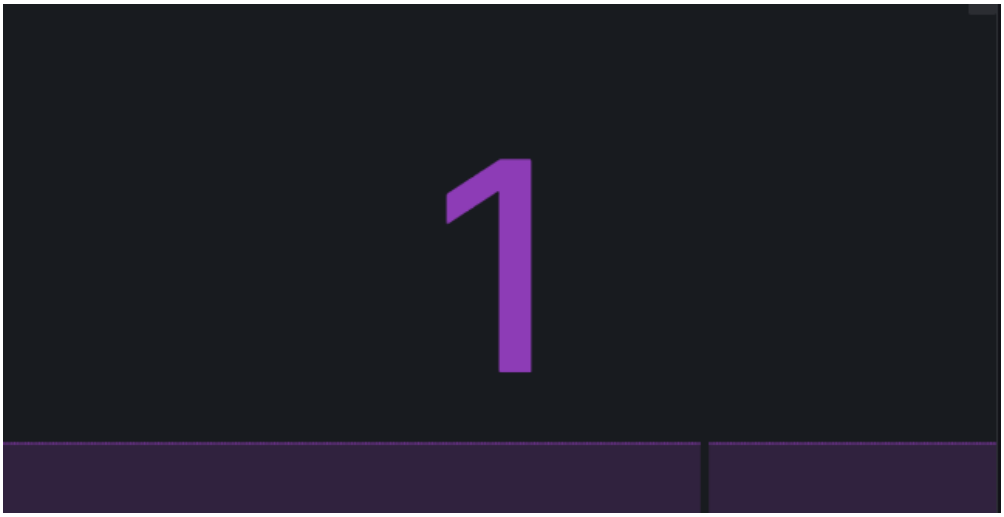
Figura 18 – Configuração do Serviço de Ping



Fonte: Autoria própria

A Figura 19 exibe um indicador numérico que reflete o status de um servidor: "1" significa que o servidor está operacional (UP), enquanto um "0" indicaria que o servidor não está respondendo (DOWN).

Figura 19 – Número de Ping

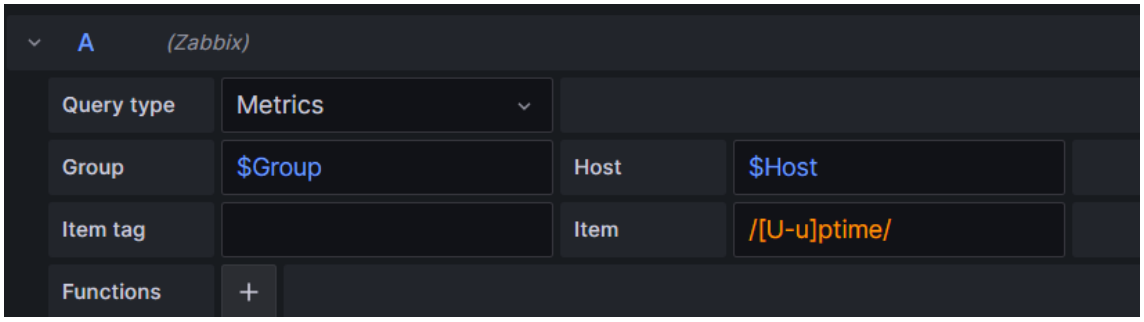


Fonte: Autoria própria

5.7 Quanto tempo um servidor está ligado

A configuração na Figura 20 mostra como e feito a verificação de tempo ligado utilizando o Grafana. A consulta é feita no serviço *Uptime*. As variáveis *Group* e *Host* são utilizadas para permitir a seleção dinâmica de grupos e hosts dentro do Zabbix, permitindo uma verificação detalhada e específica do uso da leitura e escrita nos servidores monitorados.

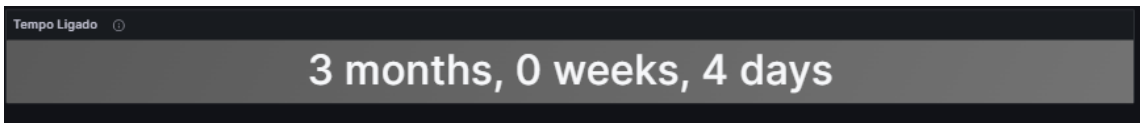
Figura 20 – Verificar o tráfego na rede



5.8 Quanto tempo um servidor está ligado

A Figura 21 informa que o servidor está ativo e operando continuamente há 3 meses e 4 dias, sem reinicializações ou interrupções no serviço.

Figura 21 – Tempo ligado

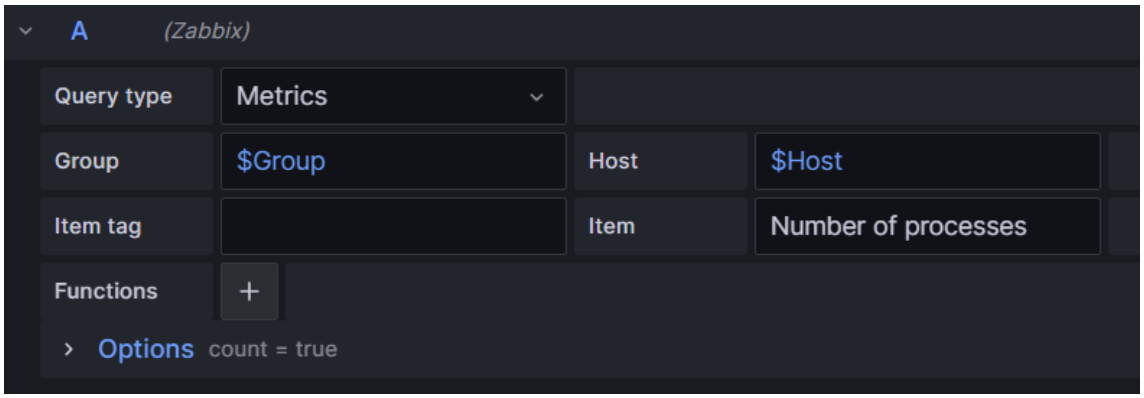


Fonte: Autoria própria

5.9 Número de Processos sendo executados no Servidor

A configuração na Figura 22 mostra como e feito para observar o número de processos com o Grafana. A consulta é feita com métricas do serviço *Number of processes*. As variáveis Group e Host são utilizadas para permitir a seleção dinâmica de grupos e hosts dentro do Zabbix, permitindo uma verificação detalhada e específica do uso da leitura e escrita nos servidores monitorados.

Figura 22 – Número de processos rodando

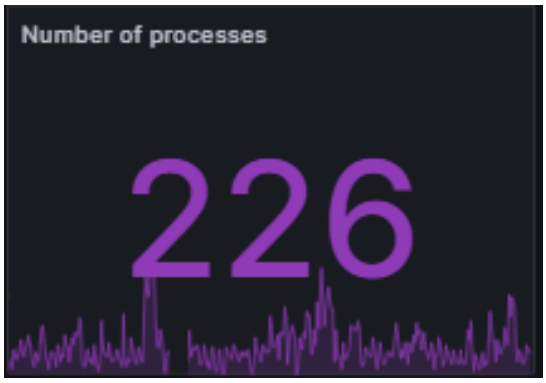


Fonte: Autoria própria

5.10 Número de Processos sendo executados no Servidor

A Figura 23 exibe que, atualmente, há 226 processos em execução no servidor. Este número é um indicativo da carga de trabalho que o servidor está gerenciando quando a métrica foi capturada.

Figura 23 – Quantidade de Processos

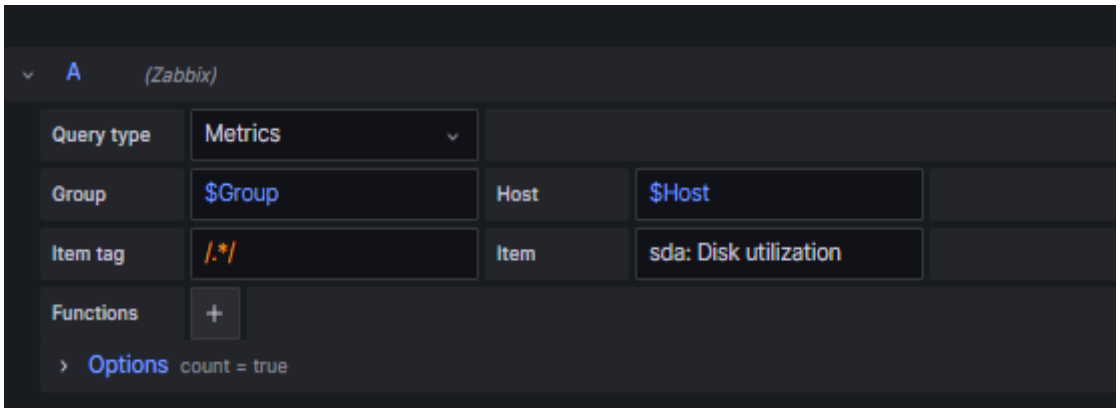


Fonte: Autoria própria

5.11 Verificar a utilização de Discos

A configuração mostrada na Figura 24 indica como verificar a utilização do disco no Grafana, utilizando a fonte de dados do Zabbix. A consulta é especificada para coletar métricas da utilização do disco identificado como 'sda'. As variáveis Group e Host são utilizadas para permitir a seleção dinâmica de grupos e hosts dentro do Zabbix, permitindo uma verificação detalhada e específica do uso do disco nos servidores monitorados.

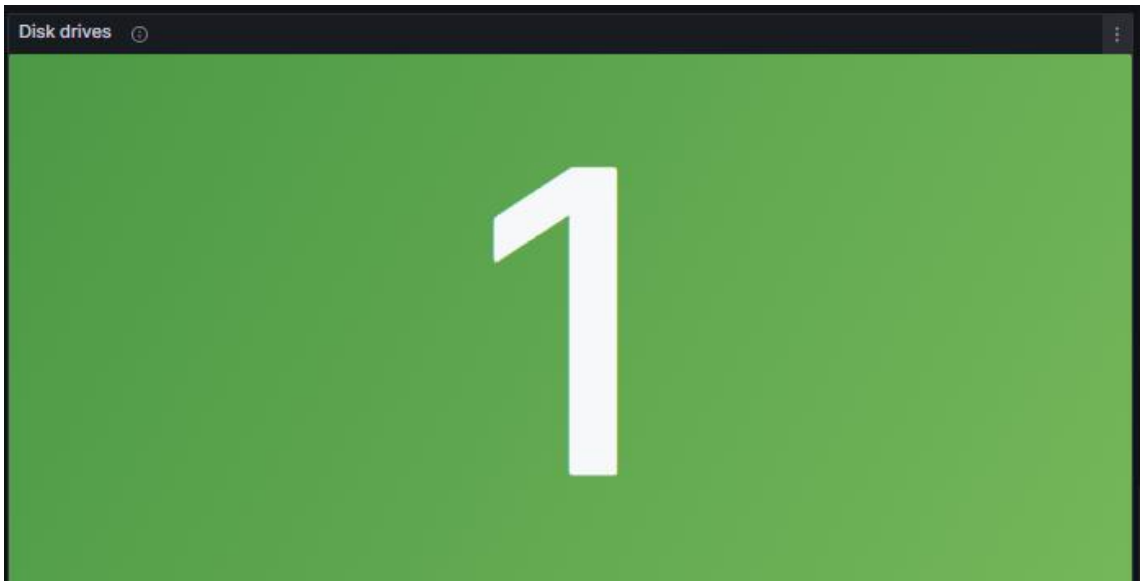
Figura 24 – Configuração de Disco



Fonte: Autoria própria

A Figura 25 apresenta a quantidade de discos físicos em uso na máquina virtual, que é indicada pelo número 1 no gráfico. Isso significa que há um disco físico disponível ou em uso no sistema.

Figura 25 – Discos utilizados



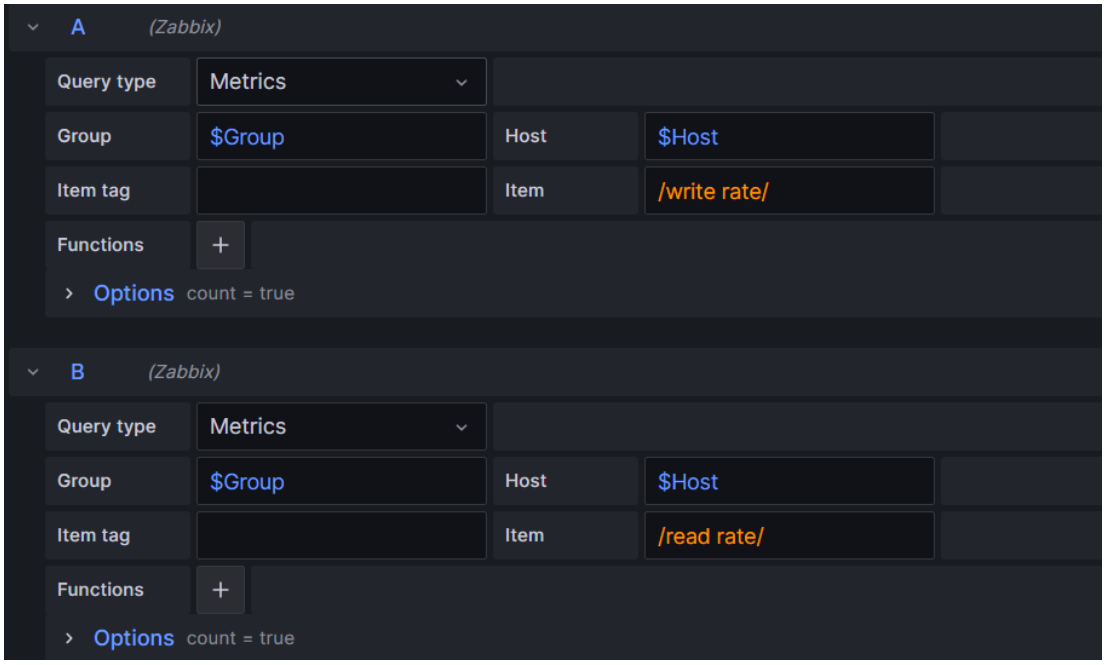
Fonte: Autoria própria

5.12 Leitura e Gravação do Disco de um Servidor

A configuração mostrada na Figura 26 mostra como e feito para verificar a saúde do disco com a leitura e gravação no Grafana, utilizando a fonte de

dados do Zabbix. A consulta é especificada para coletar métricas da utilização do disco identificado como *write rate* e *read rate*. As variáveis Group e Host são utilizadas para permitir a seleção dinâmica de grupos e hosts dentro do Zabbix, permitindo uma verificação detalhada e específica do uso da leitura e escrita nos servidores monitorados.

Figura 26 – Configuração leitura e escrita do disco



Fonte: Autoria própria

5.13 Leitura e Gravação do Disco de um Servidor

A Figura 27 exibe as taxas de leitura e escrita do disco em um servidor ao longo de um período de 5 horas.

Figura 27 – Histórico da utilização do disco

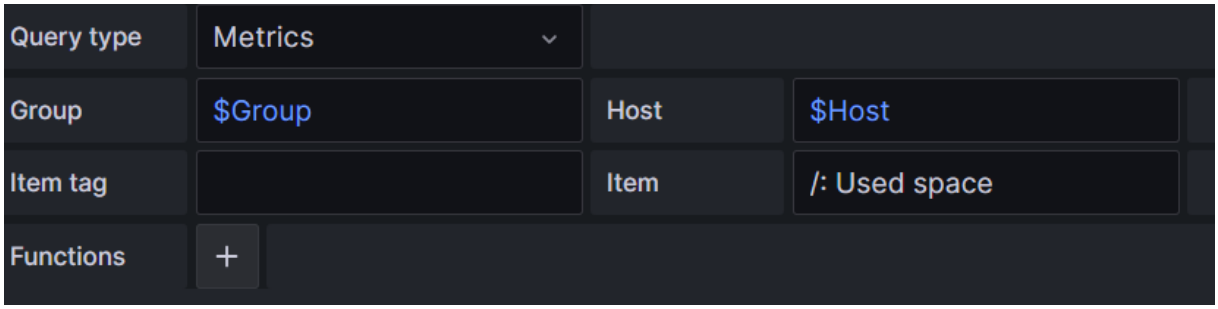
Fonte: Autoria própria

A linha vermelha representa a atividade de escrita no disco, enquanto uma linha azul (que pode não estar visível devido a uma taxa de leitura média de 0 operações por segundo) representaria a atividade de leitura. As operações por segundo (ops/s) são a unidade de medida e o pico na linha vermelha indica um aumento notável na atividade de escrita em um ponto específico do tempo monitorado. Conforme é visto, os dois picos mostrados na imagem são causados por solicitações feitas pela área de Marketing para saber se houve alteração nos dados.

5.14 Espaço Utilizado em Disco

A configuração mostrada na Figura 28 mostra como e feito para verificar o espaço do disco no Grafana, utilizando o Zabbix. A consulta é especificada para coletar a utilização do disco identificado como *Used space*. As variáveis Group e Host são utilizadas para permitir a seleção dinâmica de grupos e hosts dentro do Zabbix, permitindo uma verificação detalhada e específica do uso da leitura e escrita nos servidores monitorados.

Figura 28 – Configuração de verificação do espaço no disco

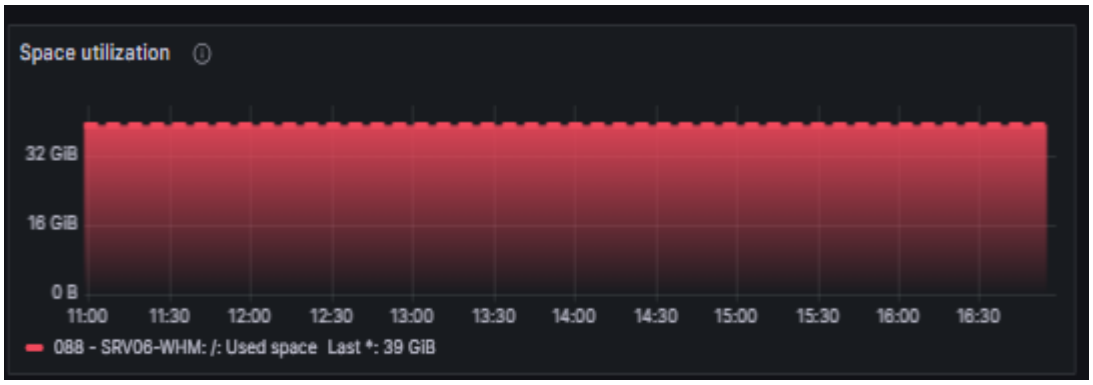


Fonte: Autoria própria

5.15 Espaço Utilizado em Disco

A Figura 29 ilustra o gráfico de utilização de espaço em disco ao longo de um intervalo de 5 horas e 30 minutos.

Figura 29 - Espaço utilizado do servidor



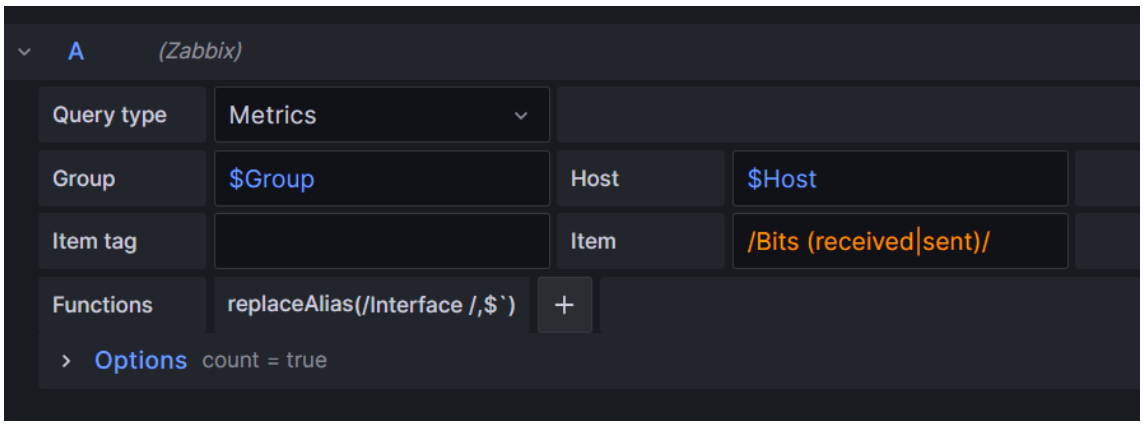
Fonte: Autoria própria

A linha vermelha representa a atividade de escrita no disco, enquanto uma linha azul (que pode não estar visível devido a uma taxa de leitura média de 0 operações por segundo) representaria a atividade de leitura. As operações por segundo (ops/s) são a unidade de medida e o pico na linha vermelha indica um aumento notável na atividade de escrita em um ponto específico do tempo monitorado.

5.16 Navegação

A configuração na Figura 30 mostra como e feito para visualizar o tráfego na rede utilizando o Grafana. A consulta é observa e coletar métricas do serviço *Bits* recebidos e enviados. As variáveis Group e Host são utilizadas para permitir a seleção dinâmica de grupos e hosts dentro do Zabbix, permitindo uma verificação detalhada e específica do uso da leitura e escrita nos servidores monitorados.

Figura 30 – Verificar o tráfego na rede



Fonte: Autoria própria

5.17 Navegação

A navegação trata-se que está trafegando na rede.

A Figura 31 traz um gráfico de rede que mostra duas métricas de atividade: a linha verde representa a taxa de bytes recebidos pela máquina ao longo do tempo, enquanto a linha roxa indica a taxa de bytes enviados. Isso fornece uma visualização do tráfego de entrada e saída da rede do servidor durante o intervalo de tempo apresentado.

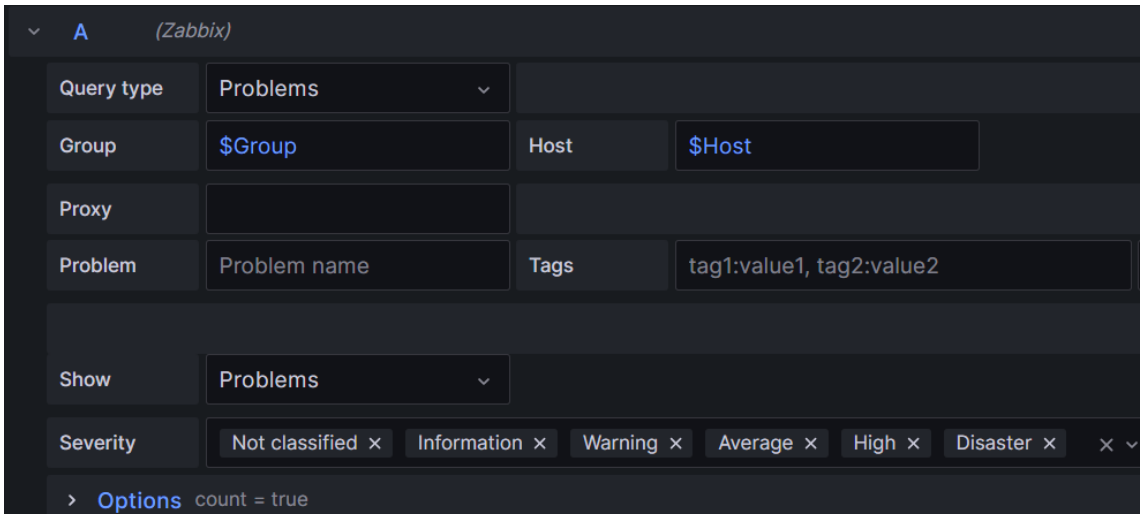
Figura 31 – Tráfego na rede

Fonte: Autoria própria

5.18 Problemas no Servidor

A configuração na Figura 32 mostra como utiliza para verificar os problemas atuais que está tendo no servidor ou sistema no Grafana. A consulta é observa e mostra os erros atuais no servidor. As variáveis Group e Host são utilizadas para permitir a seleção dinâmica de grupos e hosts dentro do Zabbix, permitindo uma verificação detalhada e específica do uso da leitura e escrita nos servidores monitorados.

Figura 32 – Problema no Servidor

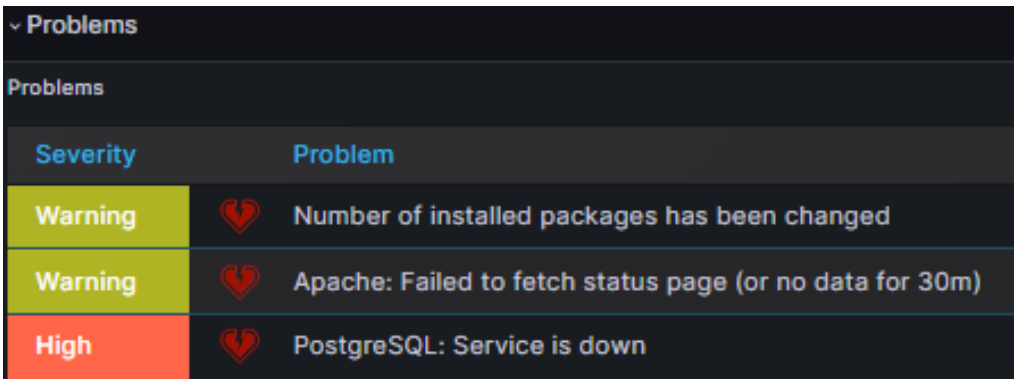


Fonte: Autoria própria

5.19 Problemas no Servidor

A Figura 33 exibe um painel de monitoramento que sinaliza problemas identificados no sistema.

Figura 33 – Problemas no servidor



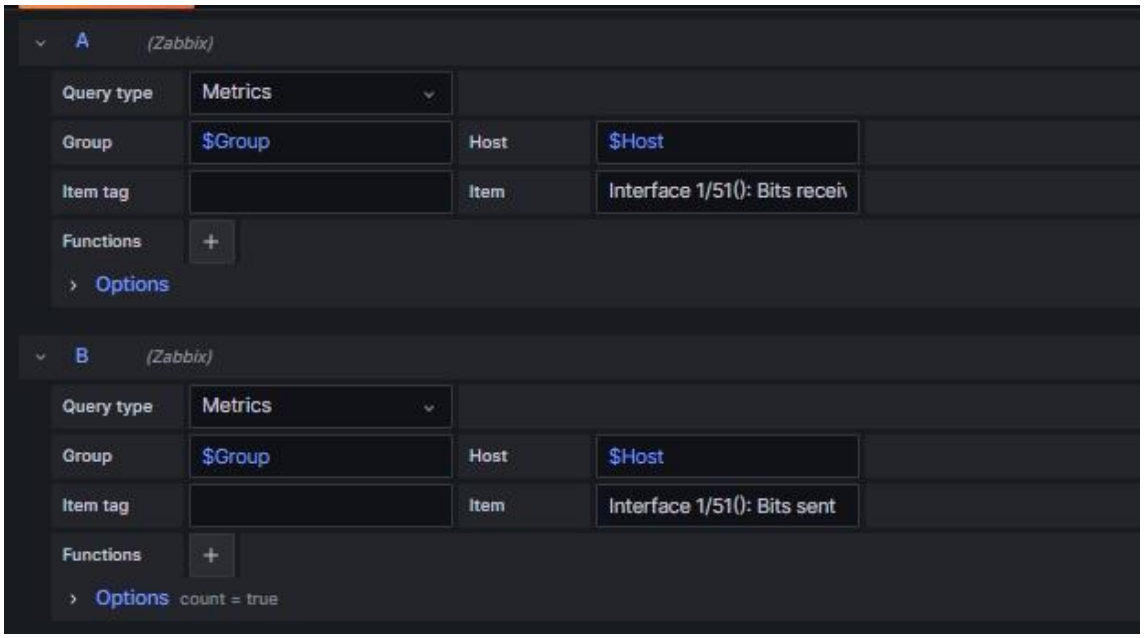
Fonte: Autoria própria

Cada problema é classificado por severidade e descrição, ajudando o administrador de rede a identificar e priorizar as questões para resolução. Os problemas listados na Figura 33 incluem uma mudança no número de pacotes instalados e uma falha em obter a página de status do Apache. Ambos classificados como advertências, enquanto um problema mais sério é destacado em vermelho, indicando que o serviço PostgreSQL está inativo.

5.20 Configuração de Switch

A Figura 34 exibe como é feita configuração no Grafana para o monitoramento de um *switch*. Para ver os bits recebidos e enviados naquele período, e feito a configuração colocando em item a interface que gostaria que fosse feito a verificação e o que gostaria de monitorar.

Figura 34 – Configuração de Switch

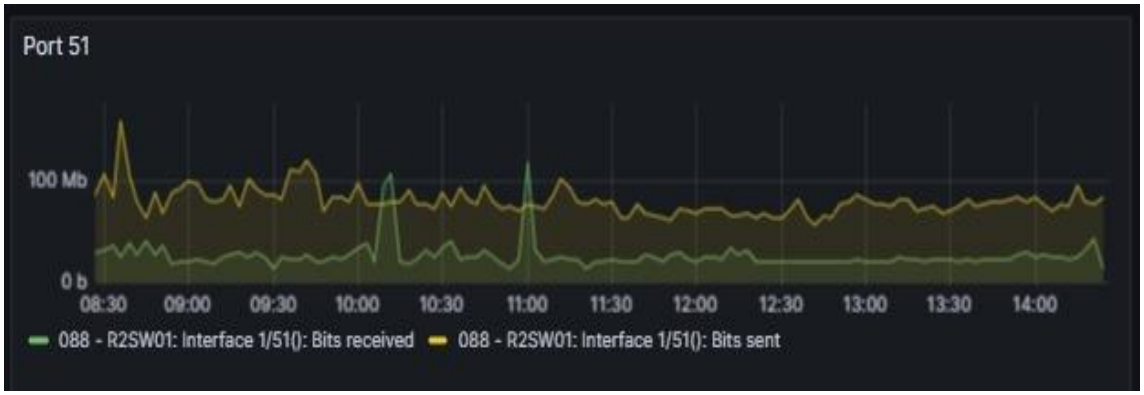


Fonte: Autoria própria

5.21 Visualização do Tráfego

A Figura 35 mostra como está sendo trafegado os dados naquele período de 6 horas

Figura 35 – Tráfego na porta do switch



Fonte: Autoria própria

Também é visto o consumo daquela porta em específico, na qual é mostrado que aquela porta está com mais tráfego de envio de informação da cor amarela, enquanto a cor verde representa os dados recebidos por aquela porta do *Switch.*

5.22 Visualização do Tráfego

A Figura 36 mostra uma visão geral do estado de várias portas de rede (conexões físicas) de um dispositivo de rede, sendo um switch. A imagem tem uma tabela organizada em fileiras e colunas. Cada célula representa uma porta conexão física no *switch.* Os status são representados em verde e vermelho onde verde representa *UP* e vermelho por *Down.*

Figura 36 – Portas do Switch

Fonte: Autoria própria

Observa-se que este switch está ligado sem problemas a 4 semanas 1 dia e 3 horas. O protocolo SNMP está como 1 o que significa que está tudo 0k. O SNMP *Agent* também está em verde e está OK.

6 CONCLUSÃO

Este trabalho tem como objetivo responder a seguinte questão de pesquisa: Como facilitar a interpretação de dados monitorados em uma rede de computadores visualizados por meio da ferramenta Grafana?

O GRAFANA serve para fazer monitoramento de rede em tempo real, com a utilização de *SNMP* por exemplo de servidores, *switches, firewalls.* Também usado para fazer alertas da rede caso haja algum problema, pode-se colocar vários *Dashboards* para melhor visualização de erros e a utilização dos processos da rede que estão sendo monitorados, o que ajuda a identificar e resolver problemas rapidamente.

Os testes realizados comprovaram que as visualizações mostradas pela ferramenta Grafana realmente facilita a compreensão e agiliza o monitoramento da rede.

Possui as vantagens de ser um serviço feito com código aberto e com uma grande comunidade, sendo possível visualizar várias formas de melhorar o sistema de monitoramento com a comunidade. Além disso, o Grafana se comunica com várias ferramentas de monitoramento, tais como o Zabbix e, com isso, melhora a visualização para o analista, por ser uma ferramenta mais interativa, facilitando a leitura dos gráficos.

Foi possível concluir que a utilização de ferramentas de monitoramento deixa a organização preparada para verificar o tráfego da rede e qual o melhor caminho a seguir com as informações que se tem. Assim, também se tem uma segurança extra, graças ao monitoramento, pois o mesmo faz uma varredura e verifica o que está sendo trafegado na rede e como está sendo esse tráfego.

Para continuidade deste trabalho sugere-se as seguintes propostas:

- Implementar a ferramenta Grafana com serviço de *Security information and event management* (SIEM) ou Gerenciamento e Correlação de Eventos de Segurança.
- Integração da ferramenta de gerenciamento e correlação de eventos de Segurança com Kubernetes.
- Integração de ferramentas como o Jenkins, no qual é feito integração com ferramenta de automação e entrega contínua.

7 REFERÊNCIAS

ANDREOLI, Y. **Análise comparativa entre ferramentas para gerenciamento e monitoramento de redes.** Trabalho de conclusão de curso de Análise e Desenvolvimento de Sistemas. Repositório da Universidade Federal do Paraná. 2016. Disponível em: <https://repositorio.utfpr.edu.br/jspui/bitstream/1/15568/1/PB_COADS_2016_2_05.pdf> Acesso em: 22 set. 2023.

Ariane G. **40 Comandos Linux Que Todo Usuário Deve Conhecer** 2023 Disponível em: <https://www.hostinger.com.br/tutoriais/comandos-linux.> Acesso em 20 de nov. 2023.

ARCENIO, L.F.S. **Monitoramento de dispositivos de redes com *Zabbix:* suas formas de coleta de informações e o custo de armazenamento**. Artigo da Universidade Federal da Grande Dourado (UFGD). 2015. Disponível em: <http://www.viiiwticifes.ufba.br/modulos/submissao/Upload-215/55153.pdf.> Acesso em: 07 out. 2023.

BONGUET, Adrien; BELLAICHE, Martine. ***A Survey of Denial-of-Service and Distributed Denial of Service Attacks and Defenses in Cloud Computing***. Future Internet, [S.L.], v. 9, n. 3, p. 43, 5 ago. 2017. MDPI AG. Disponível em: <http://dx.doi.org/10.3390/fi9030043.> Acesso em: 13 set. 2023.

BUENO, L.E.N. & WEINGARTNER, T.S. **Monitoramento de dispositivos em rede utilizando Zabbix e Grafana**. TCC - Instituto Federal Farroupilha Campus Panambi. p.149. 2022. Disponivel em <https://arandu.iffarroupilha.edu.br/bitstream/itemid/254/1/TCC%20Versao%20Final %20LUCAS%20EDUARDO.pdf.> Acesso em: 06 set 2023.

BELENTANI, L. C., MARCELLO, J. & FLORIAN, F. ***A utilização da ferramenta de monitoramento para a otimização do gerenciamento de rede.*** Revista Interface Tecnológica - Universidade Federal de Araraquara, v.15, n.2, p. 99-110. SP, 2018. Disponível em: <https://revista.fatectq.edu.br/interfacetecnologica/article/view/509/303.> Acesso em: 24 ago. 2023.

CARVALHO, L.S. **Gerenciamento e monitoramento de redes**. Projeto do curso de Ciências da Computação – UNIDERP, p.11. 2020. Disponível em: <https://repositorio.pgsskroton.com/bitstream/123456789/31698/1/LEONARDO_SARAVY_CARVALHO_ATIVIDADE-DEFESA.pdf.> Acesso em: 06 set 2023.

FABIO DOS REIS **Qual a diferença entre LAN, MAN e WAN em Redes de Dados?** 2019 Disponivel em: <http://www.bosontreinamentos.com.br/redes-computadores/qual-a-diferenca-entre-lan-man-e-wan-em-redes-de-dados/> Acesso em 20 de nov. 2023.

FERNÁNDEZ, M. P. ***Rede de Computadores.*** Editora da Universidade Estadual do Ceará (Ed. UECE). 3 ed. Fortaleza, 2019. Disponível em: <https://educapes.capes.gov.br/bitstream/capes/432730/2/Livro%20%20Introducão%20a%20Computacão.pdf.> Acesso em: 24 ago. 2023.

FORNAROLI, G.K. & ALVES, R.S. Nagios - **Monitorando a saúde de serviços, sistemas e dispositivos de rede.** Revista Interface Tecnológica, v.18 n.1. 2021. Disponível em: <https://revista.fatectq.edu.br/index.php/interfacetecnologica/article/view/1112.> Acesso em: 07 out.2023.

https://revista.fatectq.edu.br/interfacetecnologica/issue/view/24

FORNASIER, Mateus O.; SPINATO, Tiago Protti; RIBEIRO, Fernanda Lencina. ***Ransomware* e cibersegurança: a informação ameaçada por ataques a dados.** Revista Thesis Juris, v. 9, n. 1, p. 208-236, 2020. Disponível em: <https://periodicos.uninove.br/thesisjuris/article/view/16739.> Acesso em: 13 set. 2023.

GIL, A.C. **Como elaborar um projeto de pesquisa.** 6 ed. São Paulo: Editora Atlas, 2017.

GRAFANA. **Instalação do Grafana.** 2023. Disponível em: <https://grafana.com/docs/grafana/latest/setup-grafana/installation/.>Acesso em: 05 set.2023.

GRAFANA. **Instalação do Grafana no Debain ou Ubuntu**. 2023. Disponível em:<https://grafana.com/docs/grafana/latest/setup-grafana/installation/debian/.> Acesso em: 05 set. 2023.

GRAFANA **Primeiros passos com Grafana-Zabbix** 2020 Disponível em:<https://grafana.github.io/grafana-zabbix/guides/gettingstarted/#multiple-items-on-one-graph.> Acesso em: 10 set. 2023.

GRAFANA. Inicie o servidor Grafana. 2023. Disponível em:< https://grafana.com/docs/grafana/latest/setup-grafana/start-restart-grafana/.> Acesso em: 05 set. 2023.

GRAFANA. – **Sobre o Grana.** 2023. Disponível em: <https://grafana.com/docs/grafana/latest/introduction/.> Acesso em: 05 set. 2023.

GOCACHE. **O que é Grafana?** Disponível em: <https://www.gocache.com.br/dicas/o-que-e-grafana/#:~:text=O%20Grafana%2C%20sendo%20uma%20solução,de%20análise%20de%20série%20temporal.> 2021. Acesso em: 12 set. 2023.

HENTGES, R. & SCHORR, M. C. ***Monitoramento de redes de computadores utilizando o protocolo SNMP.*** Revista Destaques Acadêmicos, v. 13, n. 4, p. 145-164. 2021. Disponível em: <http://dx.doi.org/10.22410/issn.2176-3070.v13i4a2021.3037.> Acesso em: 24 ago. 2023.

Justin Ellingwood **Como usar Systemctl para gerenciar serviços e unidades do systemd** 2023 Disponível em: <https://www.digitalocean.com/community/tutorials/how-to-use-systemctl-to-manage-systemd-services-and-units-pt> Acesso em: 20 nov. 2023.

JÚNIOR, E. B. L. & NEVES, A. R. N. ***Monitoramento de redes com software livre: solução de baixo custo numa escola da rede privada***. Revista Científica Multidisciplinar Núcleo do Conhecimento. Ano 4, 5 ed., v.8, p. 17-32. 2019. Disponível em: <https://www.nucleodoconhecimento.com.br/engenharia-da-computacao/monitoramento-de-redes.> Acesso em: 24 ago. 2023.

LEANDRO. **Zabbix, o que é? Por que usar?** 2019. Disponível em: https://4infra.com.br/zabbix-o-que-e-e-por-que-usar/. Acesso em: 05 nov. 2023.

MACEDO, R. T., FRANCISCATTO, R., CUNHA, G. B. & BERTOLINI, C. ***Rede de Computadores.*** Licenciatura *em* Computação*.* Universidade Federal de Santa Maria, 1 ed. Santa Maria, 2018. Disponível em: <https://repositorio.ufsm.br/bitstream/handle/1/18351/Curso_Lic-Comp_Redes-Computadores.pdf?sequence=1&isAllowed=y.> Acesso em: 24 ago. 2023.

NETWORKING. **Melhores ferramentas de monitoramento de rede para 2023, comparadas.** 2023. Disponível em: <https://network-king.net/pt-pt/ferramentas-de-monitoramento-de-rede/.> Acesso em: 24 set. 2023.

PROFISSIONAIS DA TI. **Gestão de indicadores/métricas com Grafana**. 2018. Disponível em: <https://www.profissionaisti.com.br/gestao-de-indicadoresmetricas-com-grafana/.> Acesso em: 12 set. 2023.

SALITURO, E. **Learn Grafana 7.0**. Packt. p. 27. 2020.

SANDERS, C. & SMITH, J. **Applied Network Security Monitoring: Collection, Detection, and Analysis,** v. 1. Syngress. USA, p. 2-3. 2014.

SILVA, A.M.F & SOUZA, S.B. **Monitoramento de Redes utilizando Cacti e PHP Weathermap em equipamentos de baixa demanda de recursos.** Artigo da Universidade Estadual do Piauí (UESPI). Parnaíba -PI. 2019. Disponível em: <https://repositorio.uespi.br/bitstream/handle/123456789/156/02%20-%20BIBLI.%20COR%20-%20ANDREIVER%20MATEUS%20FERREIRA%20SILVA_PHB_CIENC.COMPUT_2019_002.pdf?sequence=1&isAllowed=y.> Acesso em: 07 out. 2023.

SCHULTZ, F. **Segurança Cibernética: o que é e como ser um especialista no assunto**. 2020. [Online]. Disponível em: <https://milvus.com.br/seguranca-cibernetica-o-que-e/.> Acesso em: 13 set. 2023

TANENBAUM, A.S. **Redes de computadores. 6** ed. Pearson. 2021.

TEIXEIRA, Cleyson Fernando Araújo. **Segurança cibernética em redes modernas: como proteger e mitigar ataques cibernéticos**. Trabalho de conclusão de curso – Universidade Federal de Ouro Preto. Ouro Preto. 2021. Disponível em: <https://monografias.ufop.br/bitstream/35400000/3567/1/MONO GRAFIA_Seguran%c3%a7aCibern%c3%a9ticaRedes.pdf.> Acesso em: 13 set. 2023.

WAZLAWICK, R.S. **Metodologia da Pesquisa para Ciência da Computação**. 2ª ed. [S.l]:Rio de Janeiro Campus.2014.

PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
GABINETE DO REITOR

Av. Universitária, 1069 ● Setor Universitário
Caixa Postal 86 ● CEP 74605-010
Goiânia ● Goiás ● Brasil
Fone: (62) 3946.1000
www.pucgoias.edu.br ● reitoria@pucgoias.edu.br

RESOLUÇÃO n° 038/2020 – CEPE

ANEXO I

APÊNDICE ao TCC

Termo de autorização de publicação de produção acadêmica

O estudante Gabriel de Castro Gonçalves do Curso de Ciencia da Computação, matrícula 2019100280081, telefone: 62 981797652 e-mail gabrielcastrog17@hotmail.com, na qualidade de titular dos direitos autorais, em consonância com a Lei nº 9.610/98 (Lei dos Direitos do Autor), autoriza a Pontifícia Universidade Católica de Goiás (PUC Goiás) a disponibilizar o Trabalho de Conclusão de Curso intitulado Grafana como uma ferramenta de visualização de monitoramento de redes de computadores, gratuitamente, sem ressarcimento dos direitos autorais, por 5 (cinco) anos, conforme permissões do documento, em meio eletrônico, na rede mundial de computadores, no formato especificado (Texto(PDF); Imagem (GIF ou JPEG); Som (WAVE, MPEG, AIFF, SND); Vídeo (MPEG, MWV, AVI, QT); outros, específicos da área; para fins de leitura e/ou impressão pela internet, a título de divulgação da produção científica gerada nos cursos de graduação da PUC Goiás.

Goiânia, 22 de JUNHO DE 2024.

Assinatura do autor: gov.br Documento assinado digitalmente GABRIEL DE CASTRO GONCALVES Data: 22/06/2024 16:12:31-0300 Verifique em https://validar.iti.gov.br

Nome completo do autor: Gabriel de Castro Gonçalves

Assinatura do professor–orientador: _ gov.br Documento assinado digitalmente SOLANGE DA SILVA Data: 22/06/2024 16:38:51-0300 Verifique em https://validar.iti.gov.br _____

Nome completo do professor-orientador: SOLANGE DA SILVA