REVISTA
Interdisciplinar da Meta

SERVIÇO PARA MONITORAMENTO DE QUALIDADE DE LINK DE *INTERNET*

INTERNET LINK QUALITY MONITORING SERVICE

João Paulo Cuba de Souza[1]
Wallison Alves Nunes[2]
Samir Patrice Batista da Silva[3]
Sérgio Clayton Viana Pinheiro[4]

RESUMO: A *internet* é uma rede complexa e em constante evolução, devido a isso, identificar falhas ou problemas pode ser um desafio para seus utilizadores, pois muitas vezes, este não tem o conhecimento necessário para compreender o funcionamento, consequentemente, em diversos casos têm dificuldade para tomar a melhor decisão quanto as providências cabíveis. Além disso, há casos onde o usuário simplesmente precisa possuir informações a respeito da qualidade do *link* de *internet*, fornecido pela provedora de *internet* por necessidades profissionais. Dessa forma, se mostra necessária uma solução para monitoramento da qualidade do *link* de *internet*, independente do cenário. Como solução, o presente estudo apresenta uma maneira de realizar o monitoramento utilizando *hardware* e *software* dedicados, especificamente raspberry como *hardware*, e zabbix e grafana como *software*, que apresente estatísticas de uso e as métricas de qualidade mais comuns quando se trata de conexão com a *internet*.
Palavras-chave: *Internet*. Monitoramento. Raspberry. Zabbix.

ABSTRACT: The *internet* is a complex and continually evolving network. Consequently, identifying faults or problems can be a challenge for its users, as they often lack the necessary knowledge to comprehend its functioning. Consequently, in various cases, they face difficulty in making the best decisions regarding appropriate actions. Additionally, there are instances where users simply need information about the quality of the *internet link* provided by their *internet* service provider for professional needs. Therefore, a solution for monitoring *internet link* quality is necessary, regardless of the scenario. As a solution, this study introduces a method of monitoring using dedicated *hardware* and *software*, specifically using a Raspberry Pi as the *hardware*, and Zabbix and Grafana as the *software*. This setup provides usage statistics and the most common quality metrics when it comes to *internet* connection.
Keywords: *Internet*. Monitoring. Raspberry. Zabbix.

INTRODUÇÃO

A *internet* é a rede global de computadores, que mantém bilhões de dispositivos simultaneamente interconectados que mudou drasticamente o modo como as pessoas se comunicam, compartilham informações e interagem. Ao longo dos anos, a *internet* evoluiu e expandiu para se tornar uma ferramenta poderosa e indispensável na sociedade, com impacto significativo em áreas como comunicação, comércio eletrônico, pesquisa, educação,entretenimento e colaboração.

[1] Acadêmico do Curso de Bacharelado em Engenharia da Computação da Faculdade de Tecnologia do Amapá – META. E-mail: jpmsap37@gmail.com
[2] Acadêmico do Curso de Bacharelado em Engenharia da Computação da Faculdade de Tecnologia do Amapá – META. E-mail: wallison1227@gmail.com
[3] Especialista em Telecomunicações – ESAB, docente do curso de Engenharia de Computação. E-mail: samir@meta.edu.br
[4] Mestre em Ciência da Computação pela Universidade Federal do Pará, docente do curso de Engenharia de Computação. E-mail: sergio@meta.edu.br

Com a crescente dependência da *internet* e das redes locais na sociedade, a falta de conhecimento e compreensão sobre esses temas pode resultar em desafios significativos para pessoas e empresas. A *internet* e as redes locais podem ser complexas e estão em constante evolução, com diversos conceitos e tecnologias envolvidas e podem ser especialmente confusas para um iniciante, porque não há nenhuma teoria de base que explique o relacionamento entre todas as partes.

Além disso, os termos técnicos são facilmente confundidos com os nomes de produtos populares. Para aumentar mais ainda a confusão, profissionais algumas vezes usam termos técnicos de uma tecnologia ao se referirem a uma característica análoga de outra tecnologia. Consequentemente, além de um grande conjunto de termos e de siglas que contêm muitos sinônimos, o jargão das redes de computadores contém termos que são frequentemente abreviados, mal-empregados ou associados com produtos (COMER, 2015).

Com isso, a ausência de coerência no campo resulta em um desafio para os iniciantes: não há nenhuma terminologia simples e uniforme para os conceitos relacionados às redes de computadores, então vários grupos tentam criar sua própria terminologia, causando aindamais desinformação (TORRES, 2004).

Comer (2015), argumenta que o monitoramento de rede desempenha um papel vital na garantia da eficiência operacional e na detecção proativa de problemas. No contexto cotidiano, os usuários dependem da conectividade para realizar tarefas essenciais, desdecomunicações básicas até processos de negócios complexos.

Permitir que os usuários monitorem o desempenho da conexão ajuda a identificar problemas potenciais e instabilidades, como alta latência e perdas de pacotes. Isso possibilitaa tomada de medidas corretivas como a comunicação efetiva com o provedor de serviços de *Internet* (ISP).

MOTIVAÇÃO

A motivação para a implementação deste sistema é devido à falta de informação sobre os parâmetros de qualidade do *link* de *internet* contratado, pois apesar de existirem ferramentas de teste disponíveis na *internet*, estas não fornecem ao usuário um feedback com informações relevantes para tentar encontrar possíveis problemas na rede, caso o contratante tenha resultados ruins ao executar os testes.

OBJETIVO GERAL

Monitorar o desempenho do *link* de *internet* através de um sistema, que inclui *hardware* e *software* dedicado para execução do monitoramento.

OBJETIVOS ESPECÍFICOS

- Hospedar um servidor utilizando e *software* zabbix para coletar os dados obtidos doroteador;
- Utilizar *hardware* dedicado para hospedar esse sistema;
- Visualizar as informações adquiridas dos parâmetros da rede por meio de uma interface *web*.

REFERENCIAL TEÓRICO

Para compreender o funcionamento do sistema que será descrito no capítulo de materiais e métodos, é preciso possuir noções prévias sobre as ferramentas e tecnologias que serão utilizadas. Desta forma, este capítulo abordará os princípios de operação, bem como conceitos sobre os componentes que fundamentarão as bases para o sistema descrito por este trabalho de conclusão de curso.

CONCEITOS DE REDE

Uma rede física é o *hardware* (equipamentos como adaptadores, cabos e linhas telefônicas) que compõem a rede, o *software* e o modelo conceitual definem a rede lógica (IBM, 2023).

Nos capítulos seguintes, serão apresentados os conceitos de redes de computadores que compreendem a parte física e lógica, fornecendo um embasamento teórico necessário para compreender o funcionamento do monitoramento de tráfego de rede e também os princípios básicos do modelo de rede supracitado. Serão abordados temas como endereçamento IP, protocolos de comunicação, topologias de pilhas de protocolos TCP/IP.

1. Internet

O sistema de comunicação entre redes que normalmente recebe a atribuição do termo *Internet*, é baseada em protocolos de comunicação padrão, como o Protocolo de

Internet (IP) eo Protocolo de Controle de Transmissão (TCP), que possibilitam a troca de dados entre os dispositivos conectados à rede.

A autora Sousa (2009) explica que, a maioria dos sistemas operacionais e dispositivos em geral tem suporte a comunicação por meio do padrão de comunicação TCP/IP, o que

permite a comunicação entre si, e entre redes internas e externas ao ambiente onde estão em operação.

A *internet* tem sido um catalisador de mudanças sociais, econômicas e culturais em todo o mundo, permitindo a globalização, o acesso à informação, a colaboração em tempo reale a conectividade instantânea.

2. Roteador

Roteadores são pontes que operam na camada de rede do modelo OSI (Open Systems Interconnection), isso significa que os roteadores conseguem ler o datagrama IP, tendo acessoa todas as informações ali presentes, em especial os endereços IP de origem e destino. Além, é claro, de poderem receber, enviar e analisar mensagens de controle (TORRES, 2004).

Roteadores possuem duas funções básicas: permitir a conexão de duas redes diferentes e escolher um caminho a ser usado para o datagrama chegar até o seu destino. A conexãoentre duas redes diferentes é possível porque o roteador "isola" cada rede.

3. Rede Local (LAN)

Uma rede local (LAN - Local Area Network) é uma rede de computadores que abrange uma área geográfica limitada, como um escritório, uma casa, uma escola ou um campus universitário. Ela permite a interconexão de dispositivos, como computadores, servidores, impressoras, dispositivos de armazenamento, entre outros, para compartilhamento de recursos e comunicação entre os dispositivos conectados (TANENBAUM; WETHERALL,2011).

As redes locais são geralmente construídas com tecnologias de rede cabeada, como Ethernet, que utilizam cabos de rede para transmitir dados entre os dispositivos, no entanto não se limita apenas a conexões físicas.

As redes locais são amplamente utilizadas em ambientes empresariais,

educacionais e residenciais, facilitando o compartilhamento de informações, recursos e serviços entre os

dispositivos conectados. Elas podem ser usadas para fins diversos, como compartilhamento de arquivos, impressão em rede, acesso à *internet*, comunicação interna, jogos em rede e outros.

Uma rede local bem projetada e configurada pode melhorar a eficiência operacional, aumentar a colaboração entre os usuários, simplificar o gerenciamento de recursos e melhorar a produtividade. No entanto, também pode apresentar desafios, como a segurança da rede, o gerenciamento de dispositivos e a manutenção da rede.

Logo, entende-se que uma rede local é uma infraestrutura de rede que permite a interconexão de dispositivos em uma área geográfica limitada, proporcionando a comunicaçãoe o compartilhamento de recursos entre os dispositivos conectados.

4. Endereçamento de IP

O endereçamento IP (*Internet* protocol) é um sistema de numeração hierárquico que possibilita a identificação e localização de dispositivos em uma rede. O autor Comer (2016), aborda o endereçamento IP como um sistema de identificação para dispositivos em uma rede.

No padrão IPv4 (*Internet* protocol version 4), os endereços são representados por quatro conjuntos de números decimais separados por pontos (Exemplo, 192.168.0.1). Já o padrão IPv6 (*Internet* Protocol version 6) utiliza uma representação hexadecimal, composta por oito grupos de quatro caracteres separados por dois pontos (Exemplo, 2001:0db8:85a3:0000:0000:8a2e:0370:7334).

5. Pacote de dados

Para realizar a comunicação de dados entre dois dispositivos, as informações são enviadas nos chamados pacotes. Para que essas informações sejam transmitidas, geralmente elas são fracionadas em blocos ou há até mesmo uma quebra de pacotes. É a partir desse movimento que as informações são transmitidas, podendo realizar assim a telecomunicação entre duas redes.

Um pacote de dados é normalmente composto por um cabeçalho, uma área de dados e por um rodapé. Além de dados do usuário, a rede pode transportar pacotes de

controle e gerenciamento quando é necessário trocar mensagens destes tipos entre equipamentos (TORRES, 2004).

PROTOCOLOS DE REDE

Os protocolos de rede são conjuntos de regras e convenções que estabelecem a forma como os dispositivos em uma rede de computadores se comunicam e trocam informações entre si. Esses protocolos definem os procedimentos, formatos e sequências de dados necessários para a transmissão, recepção e processamento de informações em uma rede.

Os protocolos de comunicação desempenham um papel fundamental no funcionamento das redes de computadores, estabelecendo as regras e convenções que governam a troca de informações entre os dispositivos conectados. Nesta seção, serão abordados os principais protocolos de comunicação utilizados atualmente, com destaque para o TCP (Transmission Control Protocol) e o UDP (User Datagram Protocol).

O TCP é um protocolo orientado à conexão, que oferece uma comunicação confiável e baseada em fluxo. Ele estabelece uma conexão entre os dispositivos envolvidos antes de iniciar a transferência de dados, garantindo que os pacotes sejam entregues corretamente e na ordem correta. Segundo Comer (2016), o TCP utiliza um mecanismo de controle de fluxo e um sistema de janelas deslizantes para otimizar a transmissão e evitar congestionamentos na rede.

Já o UDP é um protocolo de transporte não orientado a conexão, que se destaca pela sua simplicidade e baixa sobrecarga. Diferentemente do TCP, o UDP não estabelece uma conexão prévia e não garante a entrega confiável dos pacotes. Tanenbaum e Wetherall (2011) afirmam que o UDP é amplamente utilizado em aplicações que exigem uma comunicação rápida e eficiente, como streaming de mídia e jogos online, onde a perda ocasional de pacotes não é crítica para o funcionamento adequado.

Além do TCP e do UDP, existem outros protocolos relevantes na área das redes de computadores. Por exemplo, o ICMP (*Internet* Control Message Protocol) é responsável por enviar mensagens de controle e erro na *Internet*. Segundo Forouzan (2010), o ICMP desempenha um papel crucial no diagnóstico de problemas de rede, permitindo a comunicação entre roteadores e a notificação de erros em pacotes.

Para concluir, os protocolos de comunicação, como o TCP, o UDP e o ICMP, desempenham um papel essencial na troca de informações em redes de computadores.

Cada protocolo possui suas características e funcionalidades específicas, adaptando-se a diferentes tipos de aplicações. Sendo assim, compreender e utilizar adequadamente esses protocolos é fundamental para o desenvolvimento e aprimoramento das redes de computadores, garantindouma comunicação eficiente, confiável e segura.

1. SNMP

O SNMP (Simple Network Management Protocol) é um protocolo de gerenciamento de rede que permite a coleta de informações de dispositivos de rede, como roteadores, switches e servidores, por meio de uma arquitetura cliente-servidor. Ele foi desenvolvido originalmente pela IETF (*Internet* Engineering Task Force) em 1988 e é amplamente utilizadoem redes corporativas e de provedores de serviços de *internet*.

Conforme destacam Kurose & Ross (2016), o SNMP é um protocolo baseado em mensagens que utiliza a arquitetura cliente-servidor. Os dispositivos de rede que suportam o SNMP, denominados agentes, coletam informações sobre o desempenho do dispositivo, como uso de CPU, uso de memória, tráfego de rede, entre outros, e as disponibilizam em uma estrutura hierárquica de objetos gerenciados.

Por sua vez, o *software* de gerenciamento de rede, chamado de gerente, pode consultar esses objetos gerenciados por meio de comandos SNMP, como o GET (para obter o valor de um objeto) e o SET (para alterar o valor de um objeto). O SNMP também pode ser configurado para enviar notificações (traps) para o gerente quando ocorrem eventos específicos, como falhas de dispositivo ou de rede.

O SNMP é um protocolo altamente flexível e extensível, que pode ser personalizado por meio da definição de objetos gerenciados personalizados e da utilização de MIBs (Management Information Bases) adicionais.

Além disso, o SNMP também é compatível com uma ampla variedade de dispositivos de rede e sistemas operacionais, tornando-se uma solução de gerenciamento de rede amplamente adotada (FOROUZAN, 2010).

O protocolo SNMP também apresenta algumas limitações, como a falta de segurança nativa, e a dificuldade de monitorar certos tipos de dispositivos, como dispositivos móveis e sistemas embarcados.

Dessa forma, podemos inferir que o SNMP é um protocolo de gerenciamento de rede amplamente utilizado, que permite a coleta de informações de dispositivos de rede por meiode uma arquitetura cliente-servidor. Ele é compatível com uma ampla variedade

de dispositivos e sistemas operacionais, mas apresenta algumas limitações em relação à segurança e à monitoração de certos tipos de dispositivos.

2. ICMP

O ICMP (*Internet* Control Message Protocol) é um protocolo de suporte ao IP que fornece recursos para a comunicação entre sistemas na *Internet*. Segundo Tanenbaum e Wetherall (2011), o ICMP é responsável por fornecer informações sobre erros de entrega de pacotes, congestão de rede, e outras condições que afetam a entrega de pacotes de dados.

O ICMP é um protocolo que funciona na camada de rede do modelo OSI, e pode ser utilizado para diversas finalidades, como o ping (para testar a conectividade entre dois sistemas), o traceroute (para identificar o caminho dos pacotes entre dois sistemas), e o Path MTU Discovery (para determinar o tamanho máximo dos pacotes que podem ser enviados emuma determinada rota).

De acordo com Stallings (2014), o ICMP é um protocolo simples que utiliza mensagens de controle para a comunicação entre sistemas. As mensagens ICMP são encapsuladas em pacotes IP e enviadas para o endereço IP do destino desejado. As mensagens podem ter diversos tipos, como mensagens de erro, de solicitação, e de resposta, e são identificadas por meio de um código específico.

Apesar de sua utilidade, o ICMP também apresenta alguns riscos de segurança, como ataques de negação de serviço (DoS) por meio do envio de pacotes ICMP falsificados, e a possibilidade de identificar a presença de um sistema na rede por meio de respostas ICMP. Para minimizar esses riscos, é recomendado o uso de técnicas de segurança, como o filtro de pacotes e o uso de firewalls.

MÉTRICAS DE TRÁFEGO DE REDE

O monitoramento do tráfego de rede desempenha um papel fundamental na análise e no gerenciamento eficiente de redes de computadores. A coleta de métricas de tráfego proporciona insights valiosos sobre o desempenho, a utilização e a integridade da rede. Nesta seção, serão abordadas as principais métricas utilizadas para avaliar o tráfego de rede, destacando sua importância e aplicabilidade.

Uma das métricas mais comumente utilizadas é o volume de tráfego, que

representa a quantidade de dados transmitidos entre os dispositivos conectados. Essa métrica permite identificar períodos de pico de atividade, estimar a capacidade necessária para dimensionar a rede e detectar possíveis gargalos de desempenho.

Outra métrica relevante é a taxa de transferência, que mede a velocidade com que os dados são transmitidos na rede. Conforme Tanenbaum e Wetherall (2011), essa métrica é essencial para avaliar o desempenho real da rede e determinar se ela está atendendo às necessidades de largura de banda dos usuários.

Adicionalmente, a taxa de perda de pacotes é uma métrica relevante no monitoramento de tráfego de rede. Essa métrica indica a proporção de pacotes perdidos durante a transmissão de dados. Segundo Kurose & Ross (2016), a taxa de perda de pacotes desempenha um papel crucial na avaliação da qualidade da rede, especialmente em aplicações que exigem a entrega confiável de dados, como chamadas de voz pela *Internet* e transferência de arquivos.

Mais uma importante métrica é a taxa de perda de pacotes, que indica a proporção de pacotes perdidos durante a transmissão. De acordo com Kurose & Ross (2016), a taxa de perda de pacotes é uma medida crítica para avaliar a qualidade da rede, especialmente em aplicações que requerem a entrega confiável de dados, como chamadas de voz sobre IP e transferência de arquivos.

É válido ressaltar que existem diversas outras métricas de tráfego de rede, incluindo o atraso de jitter, a largura de banda disponível e a taxa de erros de transmissão. A escolha das métricas mais relevantes depende do contexto e dos objetivos do monitoramento de rede.

Por fim, as métricas de tráfego de rede desempenham um papel crucial na análise e no gerenciamento eficiente de redes de computadores, fornecendo informações valiosas sobre desempenho, utilização e segurança. Ao coletar e analisar essas métricas, os administradores de rede podem tomar decisões embasadas para otimizar a infraestrutura de rede e melhorar a experiência dos usuários

1. Largura de banda e taxa de transferência

Andrew S. Tanenbaum (2011), explica o conceito de largura de banda como a medida da capacidade de um canal de comunicação para transportar dados, representando a quantidade de informação que pode ser transmitida em um determinado período de tempo. Ele compara a largura de banda a uma estrada, onde uma via de alta capacidade

permite o tráfego eficiente de muitos veículos simultaneamente. Analogamente, uma largura de banda maior em uma rede possibilita a transferência mais rápida e eficiente de dados.

A taxa de transferência refere-se ao quantitativo de dados que foram trafegados em um determinado intervalo de tempo. De forma resumida, é possível aferir que a taxa de transferência mede a velocidade de transmissão de dados. A unidade de medida desta grandeza é dada em bits por segundo.

A largura de banda, por outro lado, se refere a taxa de transferência máxima teórica suportada por um canal de transmissão de dados. Os cálculos assumem que o transmissor efetuará uma transferência a cada pulso de clock, sem parar, e que o receptor receberá os dados transmitidos no mesmo ritmo. Isso nunca ocorre na prática e há várias explicações para isso.

2. Perda de pacotes

Perda de pacote é o termo para quando um ou mais pacotes transmitidos falham para alcançar o destino, que gera degradação de performance em vários meios digitais. Como mencionado anteriormente, um pacote é uma pequena unidade de dados que um protocolo de rede roteia entre uma origem e um destino na *Internet* ou em qualquer outra rede de comutação de pacotes.

Para Forouzan (2010), a perda de pacotes é um fenômeno que ocorre quando pacotes de dados enviados através de uma rede não chegam ao seu destino pretendido. Essa perda pode ser causada por diversos motivos, incluindo congestionamento na rede, erros nos dispositivos de transmissão, colisões, entre outros.

Os pacotes de rede contêm pequenas quantidades de dados que normalmente incluem informações como endereço de origem e destino, protocolos ou números de identificação. Do envio de e-mails ao download de vídeos, toda atividade na *Internet* requer a transferência de pacotes.

Quando os pacotes não chegam ao seu destino, os usuários finais podem enfrentar interrupções, como serviço lento ou perda de conectividade de rede. Para usuários de redes domésticas, o serviço mais lento ou a perda de rede podem criar uma experiência de usuário ruim; e para uma empresa, os problemas de rede podem afetar as operações diárias.

Normalmente, os aplicativos que dependem do processamento de pacotes em

tempo real, como chamadas de vídeo e programas baseados em áudio, sofrerão mais quando ocorrer perda de pacotes.

i. Latência

Stallings (2013), conceitua latência de maneira geral como o atraso total que ocorre quando dados são transmitidos de um ponto a outro em uma rede. Em um cenário onde diversos computadores estão conectados a uma mesma rede local, a latência tende a ser baixa entre dispositivos comuns (como computadores pessoais, celulares e impressoras, por exemplo).

No entanto, quando esses dispositivos estão conectados por meio de rádio frequência, ou seja, redes wi-fi, costuma haver maior latência na comunicação, devido o meio apresentar barreiras maiores, como interferência eletromagnética e distanciamento do equipamento de transmissão do sinal. Existem outros fatores que podem gerar aumento na latência de rede, independente do meio de comunicação.

No cenário onde uma rede tem capacidade de transmissão de até 100 Mbits/s, e existem 10 dispositivos conectados a ela simultaneamente, e todos eles estão transferindo dados a uma taxa que não ultrapasse o limite dos 100Mbits/s a latência irá manter-se estável.

Porém, caso um dos 10 dispositivos passe a exigir sozinho 100Mbits/s, todos os outros dispositivos experienciarão uma alta latência, pois toda a capacidade da rede está sendo dedicada a atender um único dispositivo, resultando num atraso da comunicação entre os outros equipamentos conectados à rede.

ii. Jitter

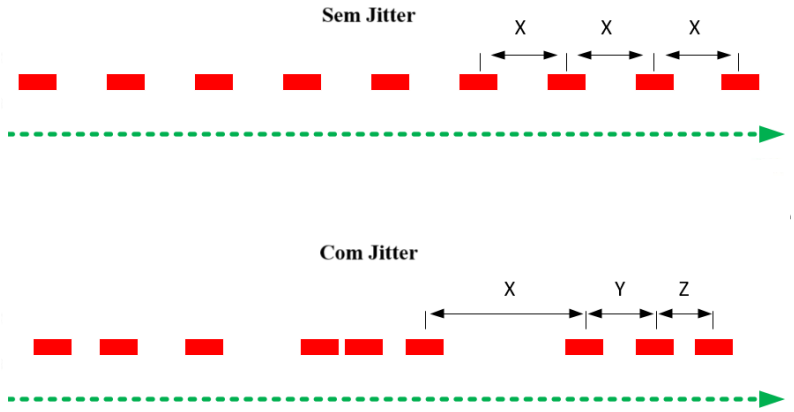
Jitter é a variação do atraso entre pacotes de dados transmitidos em uma rede, refletindo a inconsistência no tempo de chegada desse pacote dentro de um determinado período (STALLINGS, 2013). Em geral, o usuário vai notar o jitter em situações como em chamadas de voz ou vídeo. No cenário de uma transmissão de dados que precisam ser entregues completos, como o caso de um vídeo, para compensar a variação de latência durante a transmissão, normalmente o sistema lida com isso acelerando a voz ou vídeo para que o receptor receba todas as informações transmitidas.

Em jogos online é possível notar um efeito semelhante, onde todas as interações que foram perdidas durante o intervalo de tempo em que ocorria o jitter, são executadas

em alta velocidade, para que todas as informações sejam apresentadas para o usuário.

A figura 1 apresenta uma ilustração do funcionamento do jitter, os retângulos vermelhos representam os pacotes de dados. Na primeira seção da imagem vemos o tráfego depacotes sem jitter, onde todos são entregues no mesmo intervalo de tempo X. Já na segunda seção temos o jitter ocorrendo, onde os pacotes são entregues em intervalos de temposdiferentes, X, Y e Z, causando variância na latência.

Figura 1: Demonstração do funcionamento do Jitter



Fonte: https://sonary.com

DEBIAN

Para compreender o que é o debian, é necessário inicialmente possuir conhecimento mínimo sobre os conteúdos que estão atrelados ao termo “Linux”. O Linux é um kernel semelhante ao Unix disponível gratuitamente que ganhou popularidade nos últimos anos. O código-fonte do Linux está disponível publicamente, o que torna o Linux uma ferramenta atrativa para pesquisadores de ciência da computação em diversas áreas de pesquisa. Portanto, um grande número de pessoas contribuiu para o desenvolvimento do Linux (SAROLAHTI, 2002).

O Linux hoje tem milhões de usuários, milhares de desenvolvedores e um mercado em crescimento. É usado em sistemas embarcados; é usado para controlar dispositivos robóticos. Com isso, é possível agora entender o que é Debian, é uma distribuição linux de códigoaberto, que se propõe a ser uma distribuição não comercial.

Atualmente, a finalidade para a qual o sistema abordado é aplicado é para a construção de servidores de diversas naturezas, sejam servidores de arquivos, *softwares* ou mesmoserviços.

Segundo Hertzog & Mas (2020), para que essa estabilidade exista, o sistema Debian passa por um processo de desenvolvimento que se destaca em comparação a outros sistemas. Existem sempre três versões em desenvolvimento ativo do Debian: Unstable, Testing e Stable.

O motivo para a versão unstable possuir este nome advém do fato de que esta versão recebe novas funcionalidades, recursos, drivers e *software*s constantemente, bem como atualizações para os pacotes incluídos, que torna por sua vez o sistema instável, consequente do serviço de curadoria ser reduzido durante esta etapa de desenvolvimento.

A versão testing possui compilados pacotes que ainda não foram selecionados em definitivo para a versão stable, no entanto, estão em processo de debug para serem incluídos na versão stable, ou removidos em definitivo. Já a versão stable, como próprio nome sugere, é a versão mais estável do projeto, que passou por vários processos de debug, curadoria e lapidação, sendo assim a versão mais indicada para utilização em servidores (HERTZOG; MAS, 2020)

RASPBERRY

O Raspberry Pi é um computador de placa única (SBC) de baixo custo e alta versatilidade, criado pela Raspberry Pi Foundation em 2012. Ele se tornou uma ferramenta muito popular para aprendizado e experimentação em ciência da computação e eletrônica, bem como para uma ampla gama de aplicações comerciais e industriais.

O mini-computador é baseado em um processador ARM, com diferentes modelos oferecendo diferentes níveis de desempenho e recursos. Ele é capaz de executar sistemas operacionais baseados em Linux, como o Raspbian, bem como outros sistemas operacionais especializados, como o RetroPie (para emulação de videogames retro) e o Pi-Hole (para bloquear anúncios em redes).

De acordo com Monk (2023), uma das principais vantagens do Raspberry Pi é sua acessibilidade e facilidade de uso. Ele é muito mais barato do que a maioria dos computadores convencionais e requer apenas um cartão micro SD, um cabo HDMI e um teclado e mouse para começar a funcionar. Ele também é muito pequeno e portátil, o que o torna ideal para aplicações embarcadas e portáteis.

Além disso, outro ponto que vale destacar sobre o Raspberry Pi é sua flexibilidade e extensibilidade. Ele possui uma ampla gama de portas de entrada e saída (GPIO) que

permitem a conexão de uma grande variedade de dispositivos eletrônicos, como sensores, motores, displays e outros dispositivos. Ele também é compatível com uma ampla gama de acessórios e módulos adicionais, como câmeras, telas sensíveis ao toque, módulos de rádio e muito mais.

O Raspberry Pi possui uma comunidade muito ativa, de usuários e desenvolvedores, que criaram um grande acervo de recursos, tutoriais e projetos para ajudar os usuários a começar a usar e explorar o potencial do raspberry. Segundo Halfacree (2020), essa comunidade ativa e engajada é uma das principais razões pelas quais o Raspberry Pi se tornoutão popular e influente em tão pouco tempo.

Dessa forma, conclui-se que, o Raspberry Pi é uma placa de computador de baixo custo e alta versatilidade, que oferece acessibilidade, facilidade de uso e flexibilidade para uma ampla gama de aplicações.

- **ZABBIX**

Segundo a própria documentação da ferramenta, disponível no site oficial[5], Zabbix é um *software* de monitoramento de rede e aplicativos, com código aberto e licença GPL (*General Public License*), criado por Alexei Vladishev. O *software* Zabbix é essencialmente uma ferramenta de monitoramento abrangente que rastreia uma ampla variedade de parâmetros de rede, a integridade de servidores, máquinas virtuais, aplicativos, serviços, bancos de dados, sites, recursos em nuvem e muito mais. Ele emprega um sistema de notificação altamente configurável que possibilita aos usuários estabelecer alertas por e-mail para virtualmente qualquer tipo de evento, o que facilita a detecção e resposta rápida a problemas de servidor. O Zabbix também se destaca por seus recursos de geração de relatórios e visualização de dados com base nas informações armazenadas, tornando-o uma escolha ideal para o gerenciamento de capacidade.

A origem do Zabbix remonta ao final dos anos 90, quando o fundador Alexei Vladishev, trabalhando como administrador de sistemas de rede em uma grande empresa, começou a desenvolver uma ferramenta de monitoramento para gerenciar sua crescente infraestrutura de TI. Ao longo dos anos, a ferramenta evoluiu e ganhou uma ampla base de usuários e desenvolvedores em todo o mundo.

O Zabbix oferece uma ampla gama de recursos avançados, como detecção de

[5] https://www.zabbix.com/documentation/current/en/manual, acessado em 05/07/2023

problemas, análise de tendências, alertas personalizados, relatórios e visualizações gráficas, bem como suporte para protocolos de monitoramento como SNMP, SSH, ICMP, Telnet e outros. Além disso, a ferramenta é altamente escalável e pode ser facilmente configurada para monitorar ambientes de TI complexos e distribuídos, com milhares de dispositivos e aplicativos.

Desse modo, é possível dizer que o Zabbix é uma ferramenta de monitoramento de rede e aplicativos altamente flexível, escalável e de código aberto, que oferece uma ampla gama de recursos avançados para ajudar a gerenciar ambientes de TI complexos e distribuídos

- **GRAFANA**

A conceituada empresa RedHat, Inc[6] explica que o Grafana é uma ferramenta de código aberto desenvolvida pelo Grafana Labs, que oferece aos usuários a capacidade de visualizar dados de forma interativa, combinando tabelas e gráficos em um ou vários painéis, tornando mais fácil a interpretação e compreensão dos dados.

Também é possível consultar e definir alertas sobre suas informações e métricas de qualquer lugar que os dados estejam, sejam ambientes de servidor tradicionais, ou vários serviços em nuvem, etc. Assim, será possível analisar os dados com mais facilidade, identificar tendências e inconsistências e, por fim, tornar seus processos mais eficientes.

O Grafana foi construído com base nos princípios open source e na crença de que os dados devem ser acessíveis em toda a organização, não apenas para um pequeno grupo de pessoas.

MATERIAL E MÉTODOS

Tendo então finalizado a introdução aos conceitos necessários para a elaboração e montagem do sistema, o capítulo de material e métodos e seus anexos detalharão o processo de desenvolvimento do sistema e suas dependências. Para que seja possível compreender a elaboração do estudo proposto por este trabalho de conclusão de curso, algumas etapas serão exemplificadas por meio de imagens.

[6] https://www.redhat.com/pt-br/topics/data-services/what-is-grafana, 23/08/2023

- **ENTRAVES ENCONTRADOS DURANTE O DESENVOLVIMENTO**

O primeiro ponto a ser destacado, é a dificuldade de obtenção dos OID's, que são os identificadores que fornecem informações sobre os parâmetros que desejamos monitorar. A dificuldade citada está no fato de que não há informações explícitas e intuitivas, ou que forneçam com precisão a função de cada identificador, isto é, quando algum dos identificadores era fornecido, porque a maior parte da documentação disponível na *internet* não contém todas as OID's.

Esta situação forçou a procura de uma forma de visualizar os identificadores, e descobrir sua função utilizando ferramentas do mikrotik. Essa descoberta apresenta informações relevantes, pois é uma forma de documentar estes dados de OID's, que podem ser úteis a outros que estiverem procurando formas de monitorar os parâmetros capturados.

Além desse, outro empecilho que consumiu tempo e recurso dos realizadores foi a definição do *hardware* e do sistema operacional. Inicialmente foi utilizado o Ubuntu Server como S.O., no entanto, notamos que o sistema consumia muitos recursos, por possuir um elevado número de pacotes, e executar diversas atividades em segundo plano.

Dessa forma, a alternativa encontrada foi utilizar uma distribuição linux que usasse o debian como base, por apresentar um número menor de pacotes instalados e serviços em execução constante

- **HOSPEDAGEM DO SERVIDOR ZABBIX NO RASPBERRY**

Para o hospedar a ferramenta principal que fará o monitoramento dos ativos de rede, será utilizado o supracitado, raspberry, sendo ele o *hardware* onde o *software* operará coletando informações. Para utilizar o dispositivo, é necessário inicialmente instalar um sistema operacional, que preferencialmente entregue o máximo de desempenho possível consumindo o mínimo de recursos computacionais disponíveis, tais como: armazenamento, memória e CPU.

Além disso, também é importante que ele apresente um baixo uso de armazenamento, pois o sistema estará limitado a 32GB, logo, o debian se torna um sistema promissor pois apresenta pouquíssimos pacotes quando realizado uma instalação

nova. O *hardware* raspberry possui diversas versões, no caso deste projeto, o utilizado será o modelo B, de 4ª geração, com as seguintes especificações:

CPU: Quad core Cortex-A72 (ARM v8) 64-bit SoC @ 1.8GHz;
RAM: 8GB LPDDR4-3200 SDRAM;
Armazenamento: 32GB;
Interface de rede: Gigabit Ethernet;
Conectividade sem fio: 802.11ac.

O modelo utilizado não foi escolhido sem fundamento. Para atender as demandas computacionais era necessário um *hardware* robusto, e os modelos inferiores disponíveis no mercado não atendiam às expectativas de desempenho para um bom funcionamento do sistema. O zabbix foi instalado seguindo as instruções padrões disponíveis na documentação de instalação do próprio *software*, o agente, servidor e interface *web* foram instaladas juntos, sem modificações extras ou separação.

- **DIAGRAMA DA CONEXÃO DOS EQUIPAMENTOS**

Para obtenção correta dos dados e ativos de rede, é necessário montar os equipamentos e conexões de forma que o *hardware* que fornecerá dados sobre o tráfego por meio da utilização do protocolo SNMP, tenha uma interface de ligação direta com a ONT (Optical Network Terminal), equipamento fornecido pela ISP (*Internet* Service Provider) que entrega *internet* ao local. A figura 2 demonstra como será feita a conexão dos equipamentos para execução do sistema proposto por este trabalho de conclusão de curso.

O zabbix será instalado no raspberry, que terá conexão direta com o roteador interno, no caso será utilizado um equipamento da marca MikroTik, modelo HAP Lite, e este roteador fará a distribuição da *internet* recebida para os dispositivos de rede. Como o HAP Lite possui o protocolo SNMP, será possível monitorar todos os dados que trafegarem por ele por meio dozabbix.

Figura 2 - Diagrama de conexão dos equipamentos

PROCESSO DE OBTENÇÃO DE DADOS PARA MONITORAMENTO

Para monitorar ativos de rede utilizando o zabbix, é necessário a criação de itens que tenham em sua composição os parâmetros requisitados para aferição das métricas de rede. O zabbix apresenta algumas formas de realizar a captura dos itens para monitoramento, por exemplo, utilizando o protocolo SNMP, que é o principal protocolo de gerência que omikrotik é capaz de utilizar.

Como objeto de aferição, teremos as interfaces de rede do mikrotik, pois monitorando elas, será possível avaliar a conexão como um todo, devido a forma como foi organizado a rede, apresentado no capítulo anterior, na figura 2, onde todos os dados trafegados passarão por uma das interfaces do roteador, seja para entrada, ou saída.

Dessa forma, monitorando a conexão do roteador com o restante da rede, será possíveladquirir dados valiosos sobre o tráfego de rede local. Para adquirir a visualização dos itens, é necessário encontrar seus identificadores. O procedimento realizado para obtenção destes identificadores será apresentado no capítulo subsequente.

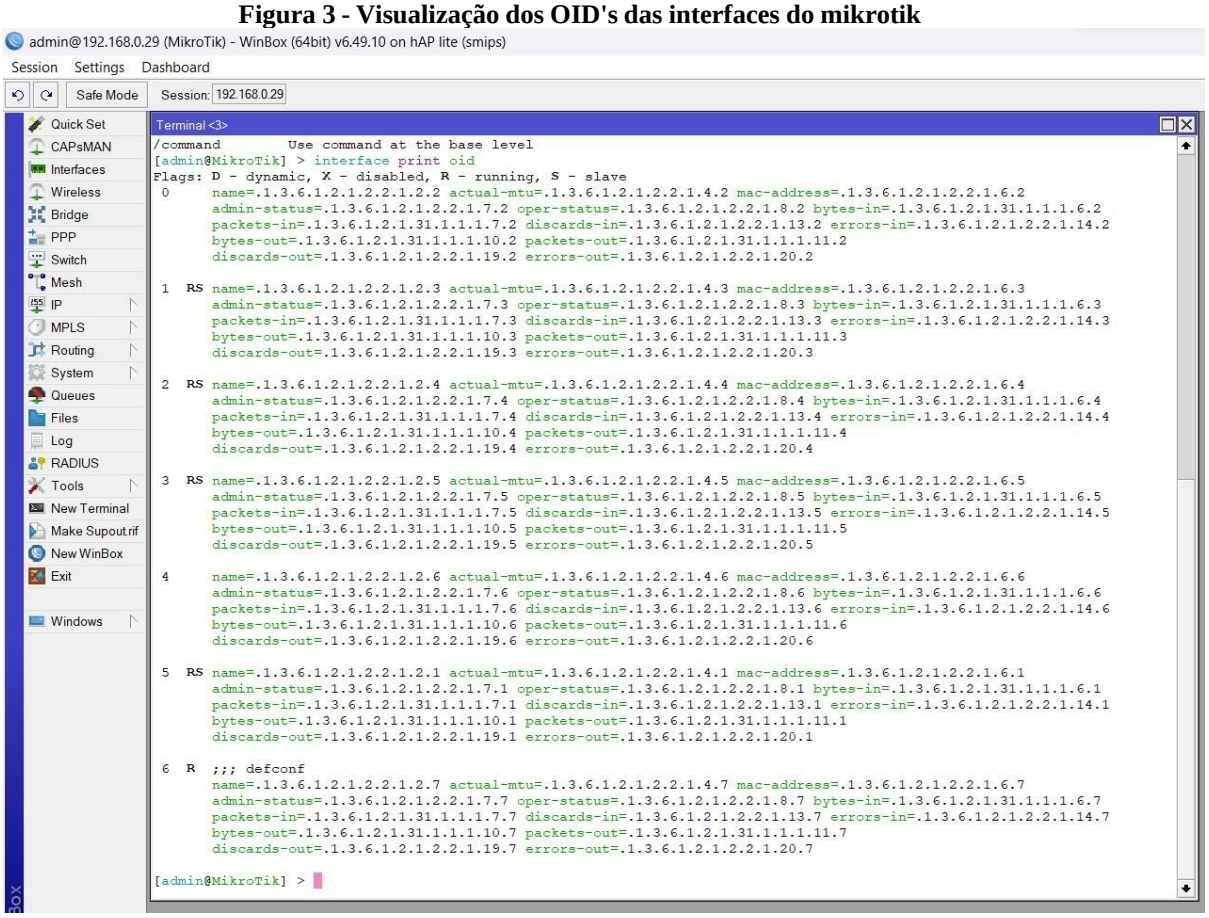
1. Obtendo dados dos itens para monitoramento

Para que seja possível realizar o monitoramento de itens de rede utilizando o protocolo SNMP, é necessário lançar uso dos OID’s(Object Identifier), que são os

identificadores de objetos em uma estrutura de gerenciamento de rede. OID's são representados numericamentecomo uma sequência de números inteiros separados por pontos, por exemplo, ".1.3.6.1.2.1.2.2.1.2.5", que é o objeto de identificação para a interface da porta 4 do mikrotik.

Para adquirir as OID's, foi utilizado o *software* WinBox, desenvolvido para o gerenciamento de dispositivos da MikroTik. Por meio do *software* citado, foi possível executar em um terminal o comando: "interfaces print oid" para visualização dos OID's de
todas as interfaces disponíveis, como demonstrado na figura 3, disponível a seguir.

Figura 3 - Visualização dos OID's das interfaces do mikrotik



Fonte: Autores (2023)

Tendo em posse os OID's, agora basta selecionar aqueles que serão necessários para o monitoramento dos itens que medirão a qualidade da rede onde o sistema será alocado. Foi optado de forma deliberada que a interface que receberia a conexão da rede local seria a interface 4, logo, precisamos monitorar os atributos da interface 4. Recolhendo informações por meio do Winbox temos 2 valores de OID's de extrema importância para o monitoramento,são eles:

bytes-in=.1.3.6.1.2.1.31.1.1.1.6.5
bytes-out=.1.3.6.1.2.1.31.1.1.1.10.5

Utilizando estes dois itens, faremos o monitoramento do tráfego geral, e da quantidadede dados trafegados na rede no período que desejarmos, utilizando o *software* zabbix.

2. Configuração do host no zabbix para monitoramento do MikroTik

Para realizar a coleta de dados no zabbix, é indispensável a criação de um host. Um host é um ativo que será monitorado na rede. Este ativo pode ser qualquer dispositivo ou sistema que possua um endereço ip, como um switch gerenciável, um celular, computador, roteador, servidor linux, um banco de dados, etc.

No zabbix, foi desenvolvido o host com as propriedades exaltadas pela figura 4 para que fosse possível monitorar o roteador mikrotik utilizado para a implementação deste projeto. Dentre os parâmetros, temos o “Host name”, que é o nome propriamente dito do hosta ser criado, este é um item obrigatório. Não é necessário para o escopo deste projeto a definição de um nome visível, mas caso fosse de interesse exibir um nome diferente do host name, esta ação poderia ser realizada inserindo informações no campo “Visible name”.

O próximo passo seria a escolha do template, no entanto, este projeto não fará uso de nenhum. Templates neste contexto são conjuntos de parametrizações definidas de formapadrão para monitoramento de alguns itens, como velocidade, latência, uso de cpu, armazenamento e outros valores. Na maioria dos casos, a utilização de templates é vantajosa, no entanto, neste projeto, não é apropriada, pois apesar de práticos, eles também têm restrições em alguns aspectos.

Com os templates não podemos alterar os parâmetros dentro dos itens já existentes, e este fator se mostrou um empecilho limitante, devido a restrições como a inabilidade de alterar a taxa de atualização da verificação de dados de cada item, a impossibilidade de adicionar regras de pré-processamento, e de verificar de que forma aquele parâmetro está sendo adquirido.

O item seguinte a ser definido é o “Host Group”. No caso, este campo determina o grupo ao qual o host estará contido. Não há maiores exigências para a determinação

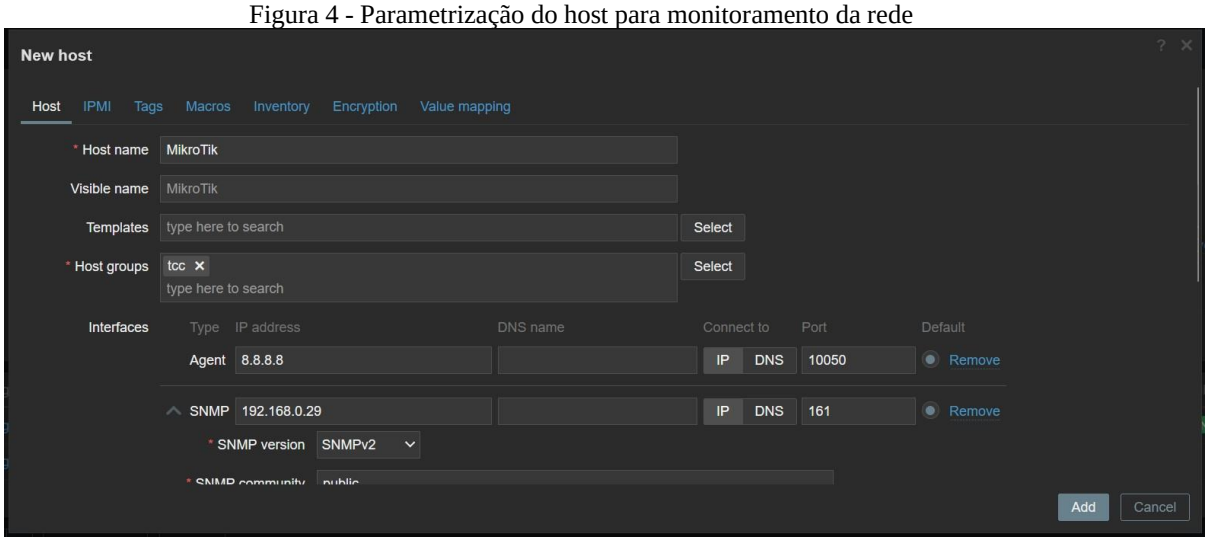
deste registo. Caso não exista um grupo, ou não queiramos usar um dos preexistentes, basta inserir o nome do novo grupo desejado no campo.

O último parâmetro que foi configurado para a criação do host são as interfaces. Para monitorar o roteador mikrotik que estamos utilizando, é necessário ter em posse a informação do endereço de IP ao qual ele está atrelado na rede. Neste caso, o IP é 192.168.0.29. Vale ressaltar que o recurso de suporte ao protocolo SNMP deve estar ativo no dispositivo que fará o monitoramento, desta forma, o tipo da interface a ser definido, também é SNMP, como demonstrado na figura 4. A porta padrão para o protocolo SNMP é 161, e foi decidido que

seria mantido ela, pois não há motivos que tornem necessário a mudança da porta na redeonde o sistema será instalado.

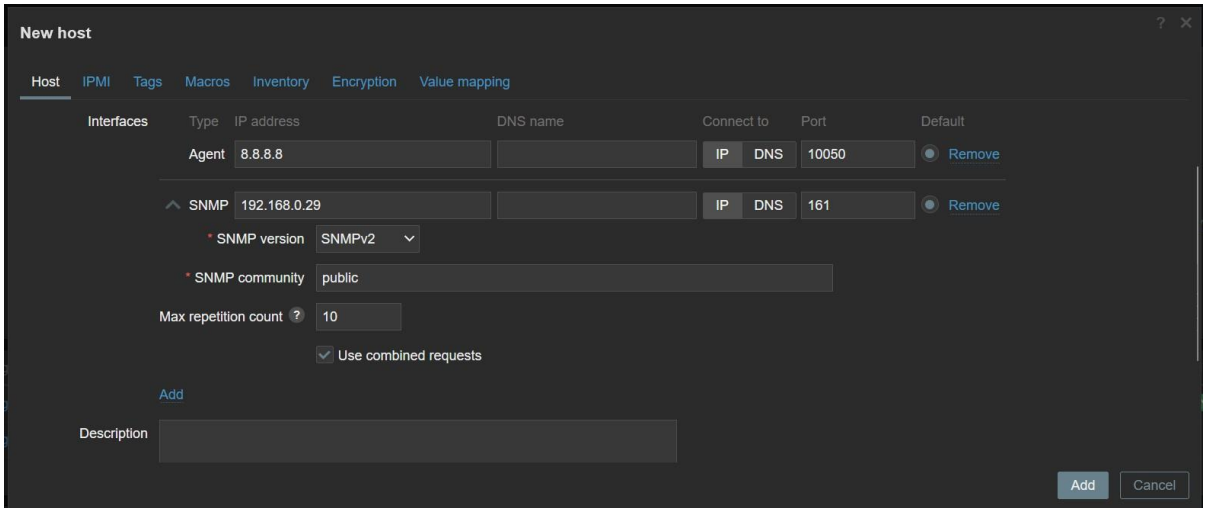
Além do mikrotik, também usaremos outra interface para mensurar parâmetros de latência de comunicação externa da rede. Para isso, utilizamos o DNS do google, o 8.8.8.8, e aporta 10050, que é a porta padrão usada para a comunicação entre o Agente Zabbix e o Servidor Zabbix.

Figura 4 - Parametrização do host para monitoramento da rede



Fonte : Autores (2023)

Figura 5 - Finalização da criação do host



Autores (2023)

A figura 5, exibida acima, demonstra os últimos parâmetros configurados para a criação do host. Para concluir, basta definir a versão utilizada do protocolo SNMP e comunidade.

Como o roteador mikrotik foi configurado com a versão 2 do protocolo SNMP, temos de definir a mesma versão para a criação do host, no caso SNMPv2. E para o campo de comunidade, também é utilizado a mesma que está definida no mikrotik, que para este sistema, é a comunidade "public". Feito isto, basta adicionar o host e a parametrização deste está concluída.

3. Configuração de itens para captura de dados

Agora que temos o host criado, devemos elaborar os itens que monitorarão os parâmetros deste host, para então exibi-los em uma dashboard. Nos subcapítulos a seguir, serão sumarizados os principais aspectos das configurações realizadas para atingir o resultado desejado de monitoramento. Para que fosse possível alcançar o objetivo, foi necessário a criação de um total de 7 itens, são eles:

1. Ehter4 (bytes_in);
2. Ehter4 (bytes_in_total);
3. Ether4 (bytes_out);
4. Ether4 (bytes_out_total);
5. ICMPPing;
6. ICMPPingLoss;
7. ICMPPingSec.

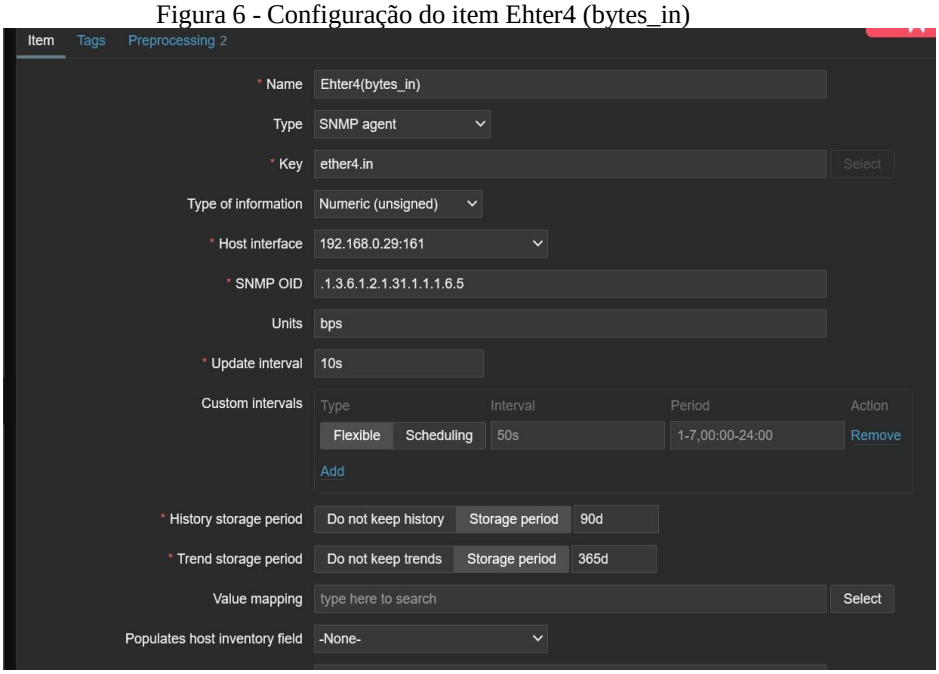
Cada um deles é de suma importância para a execução do sistema proposto por este documento acadêmico.

4. Ether4 (bytes_in) e Ether (bytes_out)

Os itens apresentados neste capítulo têm como objetivo monitorar a velocidade de download e upload da interface Ether4 do mikrotik, vale relembrar que a porta 4 é por onde o roteador recebe a conexão com a rede do estabelecimento, desta forma, monitorando parâmetros nela, é possível obter informações gerais sobre o uso de rede.

Para criação dos itens, precisamos utilizar o OID que fornece as informações sobre a variável desejada. Os OID's que serão utilizados foram citados anteriormente no subitem 3.4.1, no caso o .1.3.6.1.2.1.31.1.1.1.6.5 refere-se a dados de download, já o .1.3.6.1.2.1.31.1.1.1.10.5 fonecerá dados de upload. As telas de criação dos itens Ether4(bytes_in) e Ether4(bytes_out) são demonstrados nas figuras 6 e 7, respectivamente.

Figura 6 - Configuração do item Ehter4 (bytes_in)



Fonte: Autores (2023)

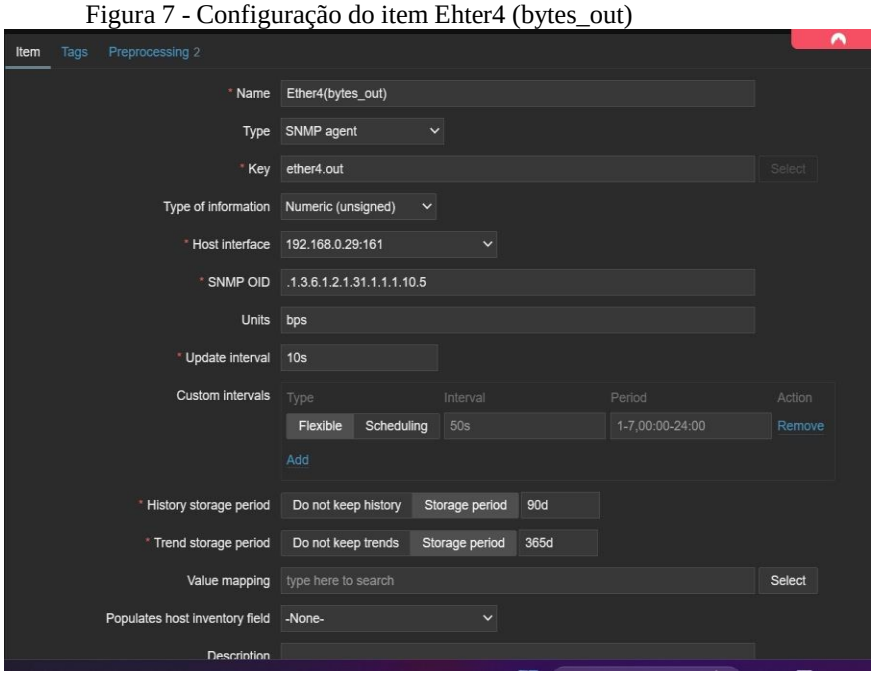
Na criação do item precisamos definir vários parâmetros, mas existem alguns que se destacam por sua importância. O parâmetro "Type" deve ser definido como "SNMP

agent", pois estamos trabalhando com esse protocolo. "Host interface" deve ser o IP definido para o roteador utilizado, em nosso caso, é o 192.168.0.29. No campo "SNMP OID" devemospreencher com o OID da variável que queremos aferir.

Foi definido que a informação capturada seria apresentada em bps (bits per second), ea atualização de coleta do item ocorreria a cada 10 segundos. Estes parâmetros foram utilizados nos dois itens de forma igual, exceto pelo OID, Foi considerado como tempo razoável 10 segundos para a consulta do item, pois quando se trata da captura de velocidade de algo, é interessante que tenhamos a informação mais próxima em relação ao tempo real possível.

Seria possível definir até 1 segundo, no entanto consultar continuamente um ativo de rede com esse intervalo exigiria mais recursos computacionais, reduzindo a escalabilidade do *hardware* utilizado. Além disso, é importante evitar consultas frequentes, uma vez que isso pode sobrecarregar os equipamentos. A constante necessidade de responder a inúmeras requisições em curtos intervalos de tempo pode resultar em problemas tanto no monitoramento quanto no acesso, comprometendo a eficiência do sistema.

Figura 7 - Configuração do item Ehter4 (bytes_out)

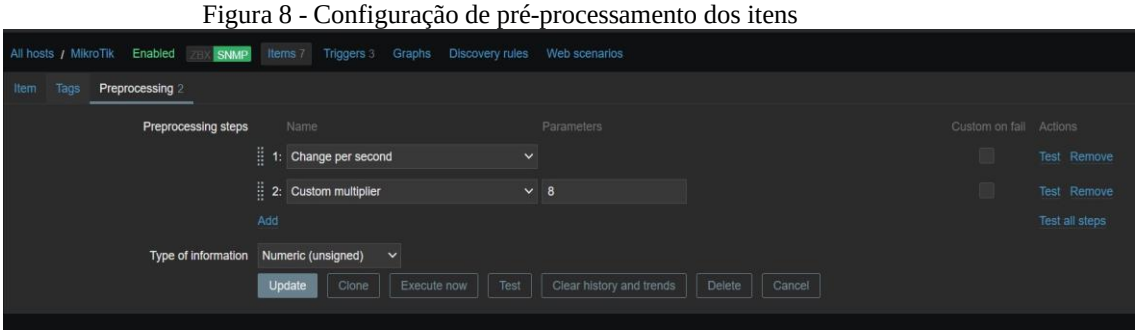


Fontes: Autores (2023)

Após criados, os itens ainda precisam de atenção, pois devemos configurar algumas funções de pré-processamento para atingir o resultado desejado. A figura 8, logo abaixo, irá ilustrar a configuração do pré-processamento, que é válido para os dois itens

criados.

Figura 8 - Configuração de pré-processamento dos itens



Fonte: Autores (2023)

É necessário configurar dois passos de pré-processamento. Primeiramente, vamos definir o passo de “Change per second”, que consiste em realizar constantemente um cálculo que verifica o novo valor, e subtrai com o valor armazenado anteriormente, obtendo desta forma, a taxa de mudança por segundo, que resulta na informação da velocidade de download e upload.

Em termos simples, caso no primeiro instante o valor armazenado fosse 600Mb, e no segundo instante, o valor é 640Mb, dessa forma sabemos que o delta entre esses valores foi de 40Mb, dessa forma, podemos aferir que a velocidade de transferência naquele instante, foi de 40Mb/s. Para melhor definição, podemos elaborar uma equação que descreve o que ocorre:

$$\text{Taxa de mudança por segundo} = \frac{X(t) - X(t-1)}{\Delta t}$$

Onde:

- $X(t)$ representa a métrica original no tempo t.
- $X(t-1)$ representa o valor da métrica original no tempo $t-1$.
- Δt é o intervalo de tempo entre as duas medições, refletindo a diferença de tempoentre t e $t-1$.

Agora que concluímos a configuração do primeiro passo, devemos adicionar como segundo, o “Custom multiplier”, que é um parâmetro de multiplicação do valor processado anteriormente. Isto deve ocorrer porque o valor obtido é dado em megabytes, e queremosobter o valor em megabits.

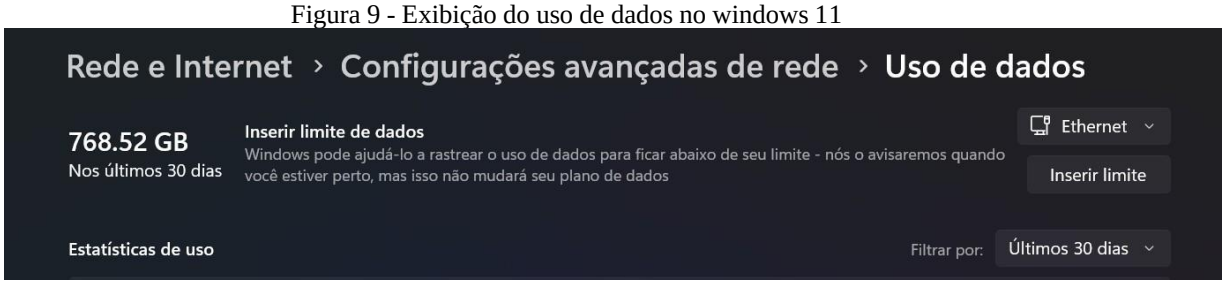
Isto se dá porque os provedores de *internet* divulgam seus planos de serviços com a unidade de medida megabits, e como a intenção do sistema proposto é fornecer informações de forma sucinta ao usuário, é interessante evitar tecnicalidades do meio, por isso, foi decidido que o valor exibido para o usuário final seria em megabits, para demonstrar que os valores condizem com o que foi contrato pelo cliente de uma ISP. Devemos realizar essa multiplicação porque um byte equivale a um conjunto de 8 bits, dessa forma, o valor do multiplicador também é 8.

5. Ether4 (bytes_in_total) e Ether4 (bytes_out_total)

Os dois itens que serão apresentados a seguir são semelhantes aos anteriores em configuração, a diferença principal é que eles não apresentam parâmetros de pré-processamento, pois a intenção destes dois itens é armazenar a quantidade de dados trafegados de upload e download para exibição do consumo de dados em um determinado período de tempo.

Diferente dos outros dois itens anteriores em que foi convertido o valor obtido para megabits, para estes outros dois, foi optado por manter o valor em megabytes, pois para consumo de dados, temos como prática comum a exibição de dados em megabytes e gigabytes. Um exemplo do cotidiano é o uso de dados no windows 11, que é exibido como demonstrado na figura 9, logo abaixo.

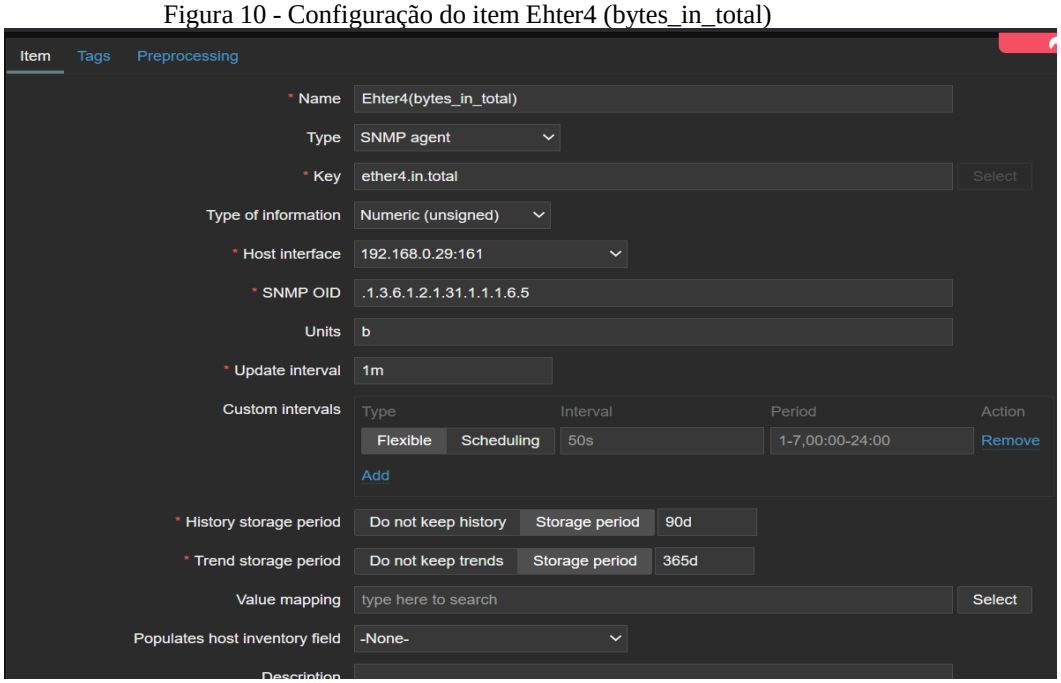
Figura 9 - Exibição do uso de dados no windows 11



Fonte: Autores (2023)

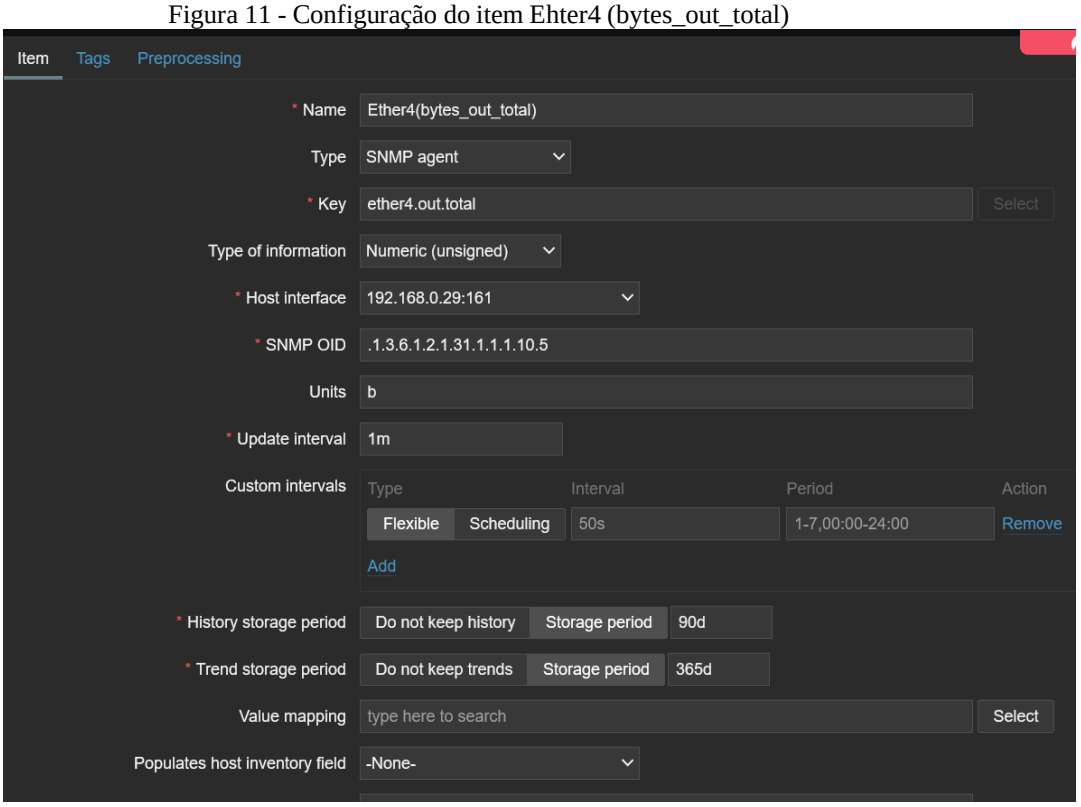
Quanto à configuração dos parâmetros, ela não difere muito dos itens criados anteriormente, já que o OID é o mesmo. É possível ver a tela de parâmetros dos itens nas figuras 10 e 11.

Figura 10 - Configuração do item Ehter4 (bytes_in_total)



Fonte: Autores (2023)

Figura 11 - Configuração do item Ehter4 (bytes_out_total)



Fonte: Autores (2023)

A principal diferença existente entre os itens deste capítulo e do anterior é em relação ao tempo de coleta de dados. Para obter a quantidade de dados trafegados ao

todo, podemos aumentar o intervalo de consultas para 1 minuto, ou até mais. Trabalhar com itens desta forma é importante, pois evita uso desnecessário de recursos computacionais do raspberry, que é de certa forma, um *hardware* com capacidade limitada.

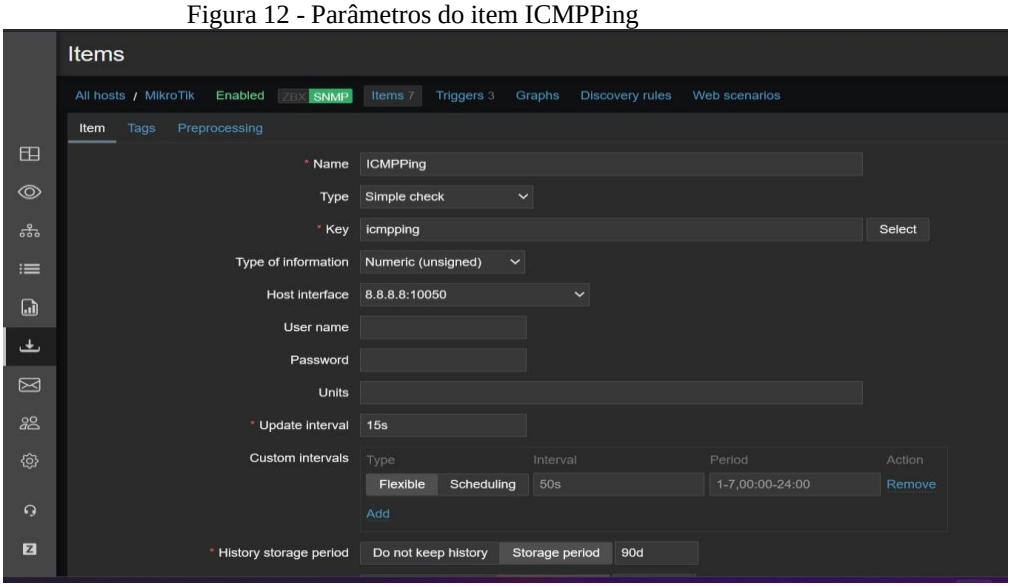
ICMPPing

O item ICMPPing, tem como função monitorar a estatística de disponibilidade de um ativo, ou um serviço. No caso deste sistema será utilizado para monitorar o serviço de DNS do google. O item vai verificar se o ativo, ou serviço neste caso, está respondendo o protocoloICMP, apresentando como resposta, uma variável booleana, que retornará o valor "1" para sucesso na resposta, porém caso a resposta seja negativa, o valor retornado é "0".

A figura 12 exibe a tela de criação do item abordado neste capítulo, demonstrando os parâmetros inseridos para o funcionamento do mesmo. Como pontos de destaque, temos o campo "Type", que está definido como simple check, pois se trata de, como o próprio nome diz, uma verificação simples, já que não é necessário nenhum outro parâmetro além do endereço de IP do serviço ou ativo que ele monitorará.

Como interface de host, utilizaremos o host que foi criado no capítulo 3.4.2, utilizando como IP o endereço 8.8.8.8. Por último, definimos o intervalo de atualização como 15 segundos, pois é um tempo razoável para verificação de conexão. O restante dos campos, não apresentam relevância para o cenário trabalho neste trabalho de conclusão de curso.

Figura 12 - Parâmetros do item ICMPPing



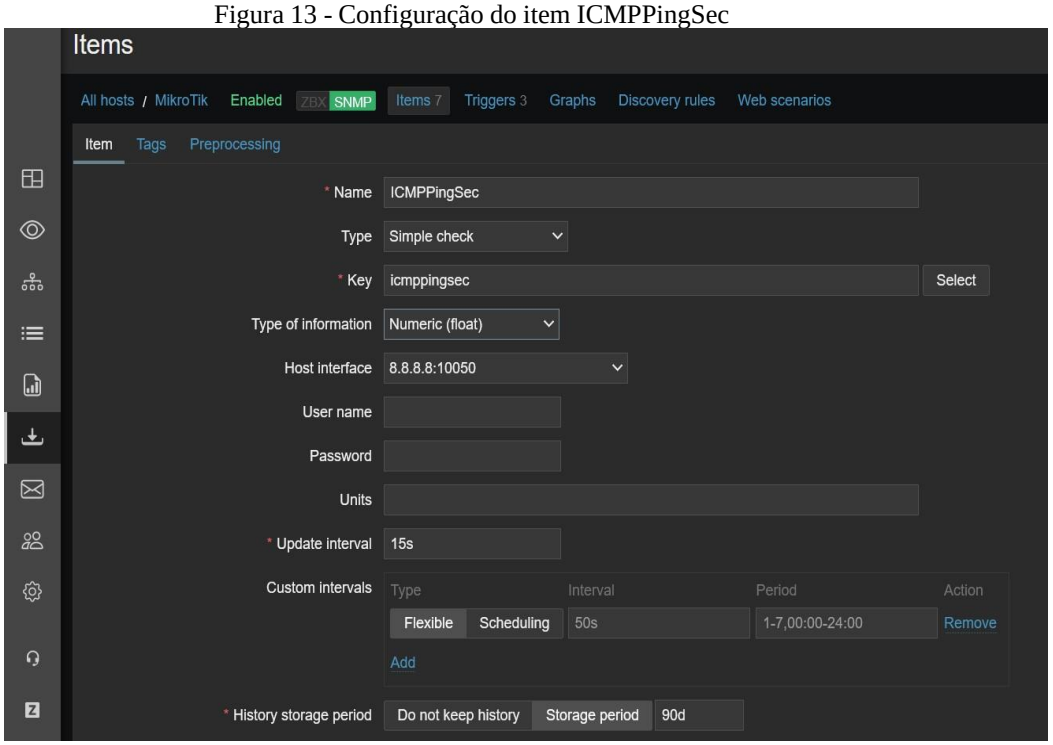
Fonte: Autores (2023

ICMPPingSec

O item ICMPPingSec mede o tempo que um serviço ou ativo leva para responder a uma requisição ao protocolo ICMP. Para mensurar o tempo que um serviço ou ativo leva pararesponder a uma requisição, utiliza-se a unidade de medida em milissegundos. Quanto maior o tempo de resposta, menor é a qualidade da conexão, devido às requisições de outrosprotocolos também levarem um tempo maior para serem atendidas.

A figura 13 abaixo demonstra a criação do item. O item basicamente utiliza os mesmos parâmetros do item anterior. A diferença é parâmetro "key", onde neste caso, é utilizado "icmppingsec" para executar a função desejada. O intervalo de atualização também foi definido como 15 segundos.

Figura 13 - Configuração do item ICMPPingSec



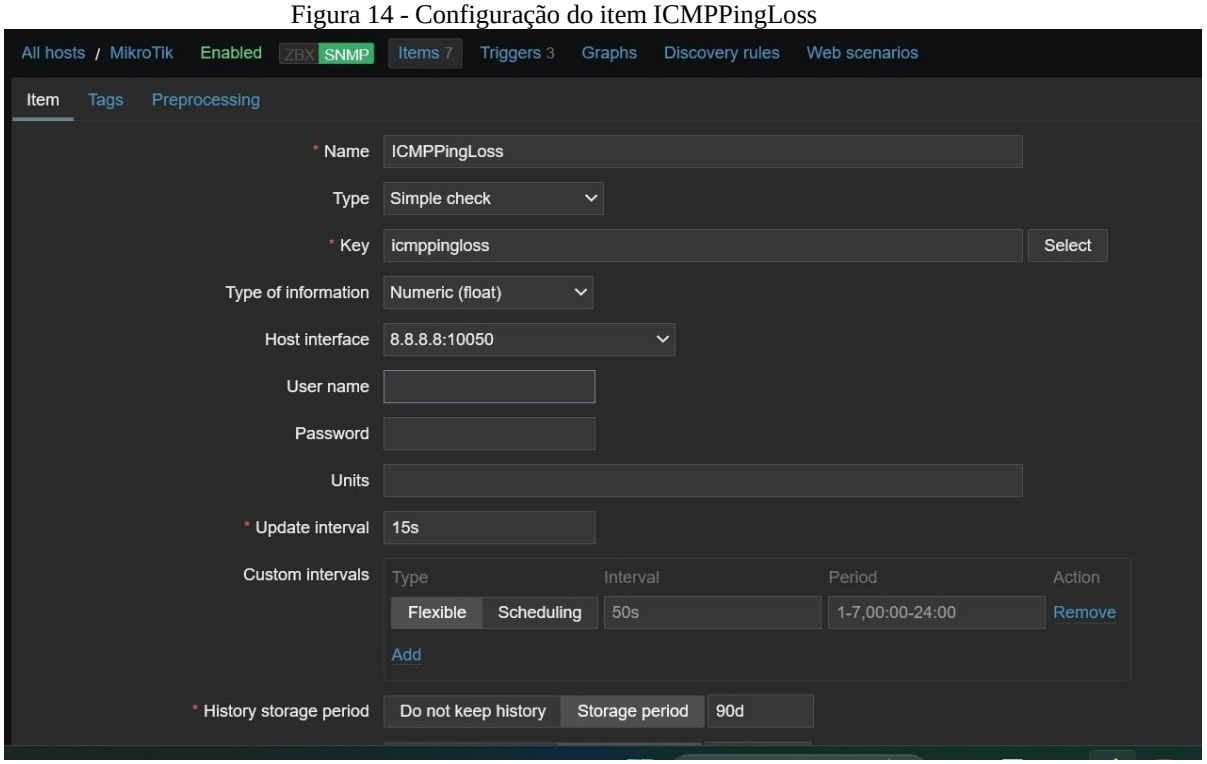
Fonte: Autores (2023)

ICMPPingLoss

O último item adicionado para fins de monitoramento é o "ICMPPingLoss". Este item tem como finalidade avaliar a qualidade da comunicação da rede com um host previamente determinado. A verificação ocorre por meio de testes com pacotes. O item utiliza o protocolo ICMP para enviar alguns pacotes para o host designado, neste caso, o DNS do Google, e aguarda a resposta.

Se forem identificadas falhas no retorno dos pacotes, o item fornece, em porcentagem, a quantidade de pacotes perdidos. A figura 14 apresenta os parâmetros definidos para a criação do item, que apresentam semelhanças com os dois itens abordados anteriormente neste capítulo.

Figura 14 - Configuração do item ICMPPingLoss



Fonte: Autores (2023)

Com isto, está encerrada a criação de itens para monitoramento, agora, a próximaetapa é desenvolver as triggers que utilizarão os itens desenvolvidos. O capítulo a seguir discorre sobre a utilidade das triggers que serão criadas, e também sobre informações pontuaisda criação das mesmas.

I. Criação de triggers

Para que alguns dos itens criados apresentem suas funcionalidades para o usuário, é preciso apresentá-los por meio de triggers, que funcionam como alertas para notificar sobre alterações em parâmetros. Segundo a documentação do zabbix, disponível no site oficial[7], as triggers constituem expressões lógicas que examinam as informações capturadas pelos itens e indicam o status do sistema, ou de um ativo, com base nesses

[7] https://www.zabbix.com/documentation/current/pt/manual/config/triggers, acessado em 05/07/2023

dados.

Foram desenvolvidos ao todo 3 triggers para tratar os dados que foram coletados, informando falha de conexão com a *internet*, saturação de banda e perda de desempenho. Cada uma será descrita nos subcapítulos a seguir.

Trigger: Sem *internet*

Esta trigger tem como intuito alertar sobre uma falha total, que ocorre quando não há resposta alguma para requisições enviadas ao DNS do google, ou seja, quando a rede local não tem acesso à *internet*.

A figura 15 demonstra os campos que devem ser preenchidos para a criação da trigger trabalhada neste capítulo. É evidente que há campos que apresentam maior importância que outros, e para deixar a explicação sucinta, serão trabalhados principalmente os pontos mais importantes. Não será discorrido sobre aquelas que não foram utilizadas.

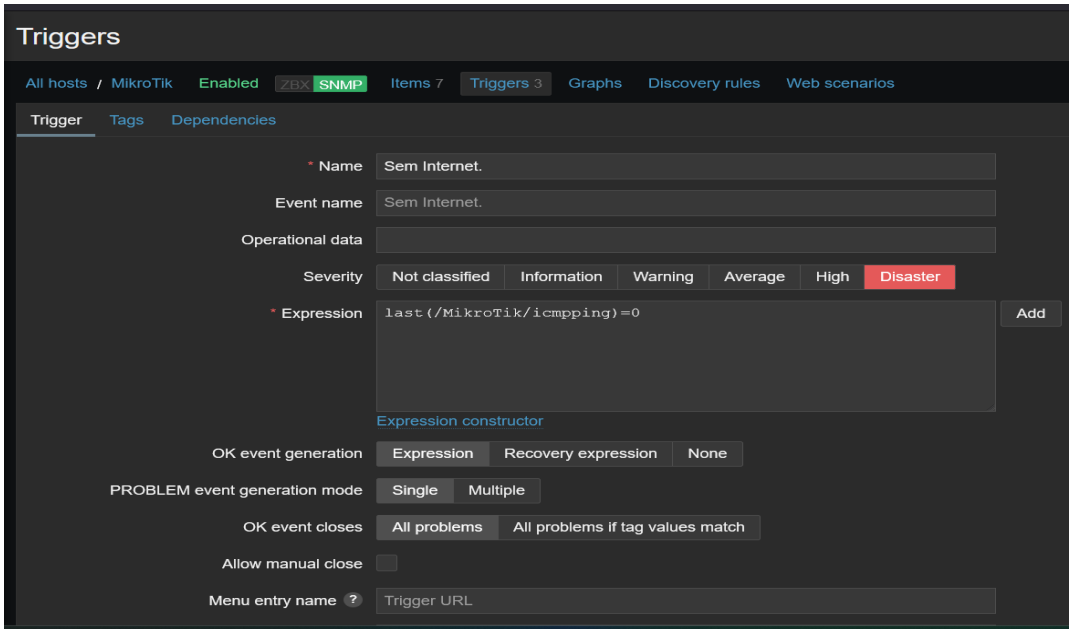
Inicialmente, temos a definição do nome da trigger, que neste caso, será: Sem *internet*.O próximo campo relevante é aquele que define o grau do alerta. Um caso onde ocorre aperda total da conexão com a *internet* é o pior dos cenários, dessa forma, o grau de severidadeda ocorrência é o mais alto existente, que no zabbix, é intitulado como “disaster”.

Por último, temos a criação da expressão, que será efetivamente a parte lógica do acionamento da trigger. A expressão utilizada foi a seguinte:

$$last(/MikroTik/icmpping)=0$$

A expressão funciona verificando o último valor (last) que foi armazenado no host selecionado para o item (Mikrotik) e o item que será avaliado (icmpping) e verifica se esse valor é igual a 0, caso seja, então é emitido o alerta.

Figura 15 - Trigger "Sem *internet*"



Fonte: Autores (2023)

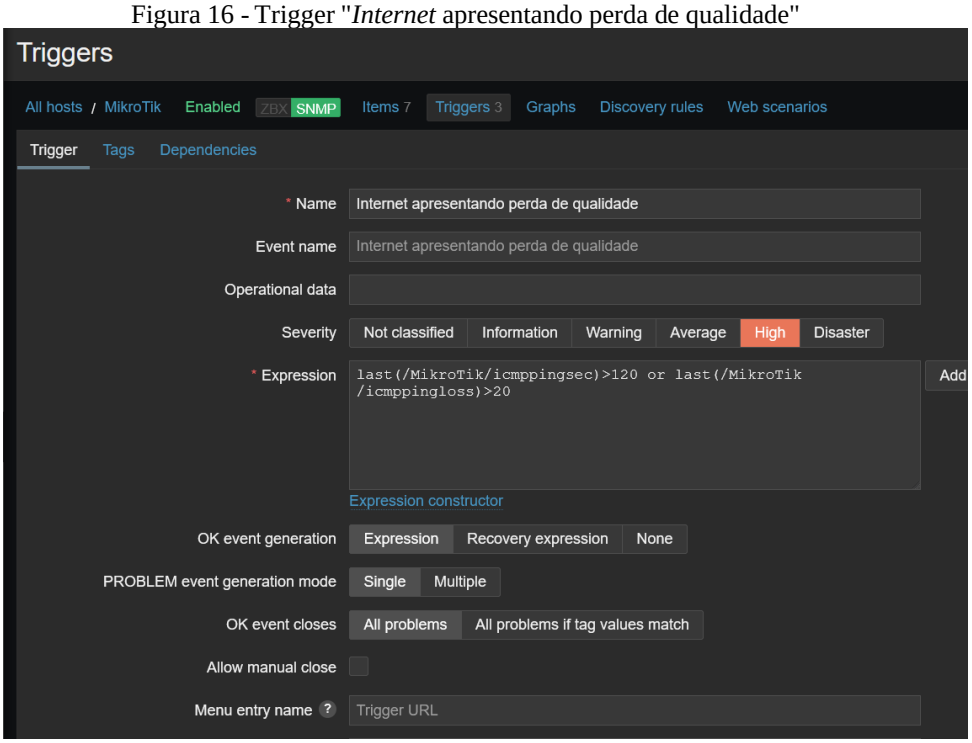
Trigger: *Internet* apresentando perda de qualidade

A trigger que será trabalhada neste capítulo tem como intuito notificar sobre perda de qualidade da conexão com a *internet*, utilizando parâmetros como a perda de pacote e alta latência. Como o cenário monitorado por esta trigger não é tão grave quanto o apresentado anteriormente, o nível de alerta definido foi alto.

Apesar de não ser uma perda total da conexão, caso a porcentagem de perda de pacotes esteja alta, em conjunto com uma latência também elevada, a junção desses dois fatores pode em alguns casos praticamente impedir o usuário de utilizar serviços que dependam de *internet*.

A figura 16 demonstra o preenchimento dos campos. O que deve receber maior atenção, é a expressão, pois ela define o modo de atuação da trigger.

Figura 16 - Trigger "*Internet* apresentando perda de qualidade"



Fonte: Autores (2023)

A expressão utilizada é dada a seguir:

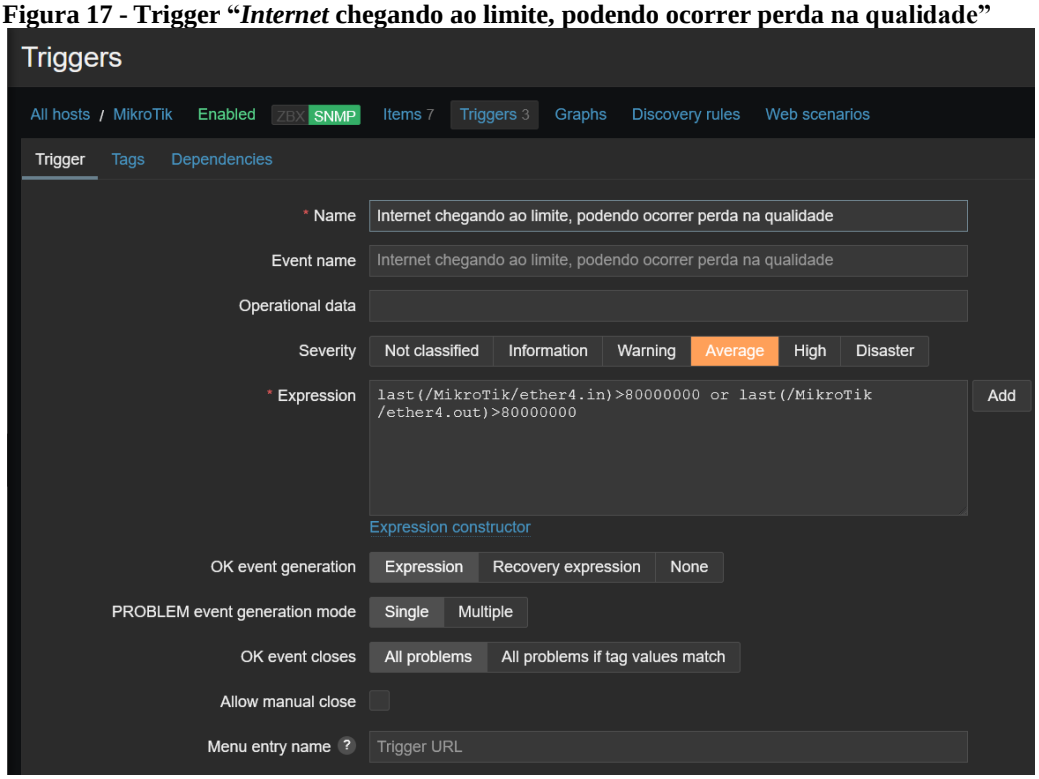
$$last(/MikroTik/icmppingsec)>120 \text{ or } last(/MikroTik/icmppingloss)>20$$

Nessa expressão, será verificado se o último valor (last) do host (MikroTik), no item (icmppingsec) é maior que 120, no caso, este valor é referente a latência, que é dada em milissegundos, ou se o último valor (last) do host (MikroTik) no item (icmppingloss) é maior que 20%. A porcentagem é referente a perda de pacotes. Caso um desses dois eventos ocorra, o alerta de perda de qualidade é disparado.

Trigger: *Internet* chegando ao limite, podendo ocorrer perda na qualidade

A última trigger criada será abordada neste capítulo. O intuito desta trigger é disparar um alerta caso seja identificado alto uso da banda contratada, pois, caso o limite seja atingido,pode elevar a latência e causar perda de pacotes. De forma geral, o usuário irá experienciar lentidão. A figura 17, abaixo, demonstra a criação da trigger.

Figura 17 - Trigger "*Internet* chegando ao limite, podendo ocorrer perda na qualidade"



Fonte: Autores (2023)

A expressão dessa trigger é a seguinte:

last(/MikroTik/ether4.in)>80000000 or last(/MikroTik/ether4.out)>80000000

O funcionamento segue um padrão semelhante ao visto na trigger anterior. Na primeira parte da expressão, é feito a verificação do último valor (last) do host (MikroTik), noitem (ether4.in) para observar se é maior que 80000000 (oitenta milhões) de bits. O valor definido está em megabits. É importante ressaltar que este valor pode ser alterado conforme o ambiente onde o sistema está instalado, e depende principalmente de dois fatores: plano de *internet* contratado e equipamentos utilizados.

A segunda parte da expressão, logo após o "or" faz a verificação do último valor (last) do host (MikroTik) no item (ether4.out) para avaliar se é maior que 80000000 (oitentamilhões) de bits.

Apesar de ser semelhante nas duas partes, há uma diferença importante: A primeira parte faz a checagem do item que armazena os valores de velocidade de download, já a segunda verifica os dados de upload, e caso qualquer um dos dois esteja

próximo de atingir o limite pré-definido, é disparado o alerta, que tem nível médio de severidade definido.

DASHBOARD PARA EXIBIÇÃO DE DADOS

Nos capítulos anteriores foram desenvolvidos meios para obter os dados de interesse para monitoramento, no entanto, não basta possuir os dados, eles precisam ser exibidos de forma que apresentem informações relevantes ao usuário, e para isso, são utilizados dashboards.

Para entendermos melhor a definição de uma dasboard, buscamos a definição de um autor: “Um painel de controle, conhecido como "dashboard", constitui uma representação visual das informações primordiais indispensáveis para atingir um ou mais objetivos. Essas informações são consolidadas e organizadas em uma única tela, possibilitando a monitorização eficiente e ágil”, adaptado de (FEW, 2006, p. 26).

Tendo essa informação em voga, quando observamos as dashboards que podem ser geradas pelo zabbix, notamos que o *software* não apresenta painéis de controle muito intuitivos, e as opções de configuração dos dados exibidos são poucas, desta forma, se fez necessário encontrar uma alternativa para exibir as informações adquiridas.

Para executar esta tarefa, foi utilizado então o *software* apresentado no capítulo de referencial teórico: Grafana. Esta ferramenta é mais bem apropriada para a tarefa de exibição de informações, pois permite maior controle da dashboard que possui, viabilizando alterações de cores, fontes, tamanho, intervalo de exibição, tipo de gráfico, entre outras opções relevantes.

1. Instalação do Grafana

Para utilizar o grafana, é necessário realizar a instalação deste em uma plataforma que irá hospedá-lo, no caso, será utilizado o raspberry, dessa forma, ele compartilhará recursos com o zabbix. Para realizar a instalação da ferramenta, basta seguir as instruções de instalaçãopara o *hardware* escolhido.

Os passos para instalação estão disponíveis na própria documentação do grafana[10]. Não foram feitas alterações que apresentassem relevância para serem citadas neste documentoem relação ao procedimento padrão de instalação.

2. Integração do grafana ao banco de dados do Zabbix

Para que o Grafana exiba as informações que estão armazenadas no zabbix, é preciso realizar a integração de uma ferramenta à outra. Para realizar esta tarefa, o primeiro passo é executar a instalação do plugin que realiza a conexão com o zabbix.

Figura 18 - Plugin para conexão com o zabbix

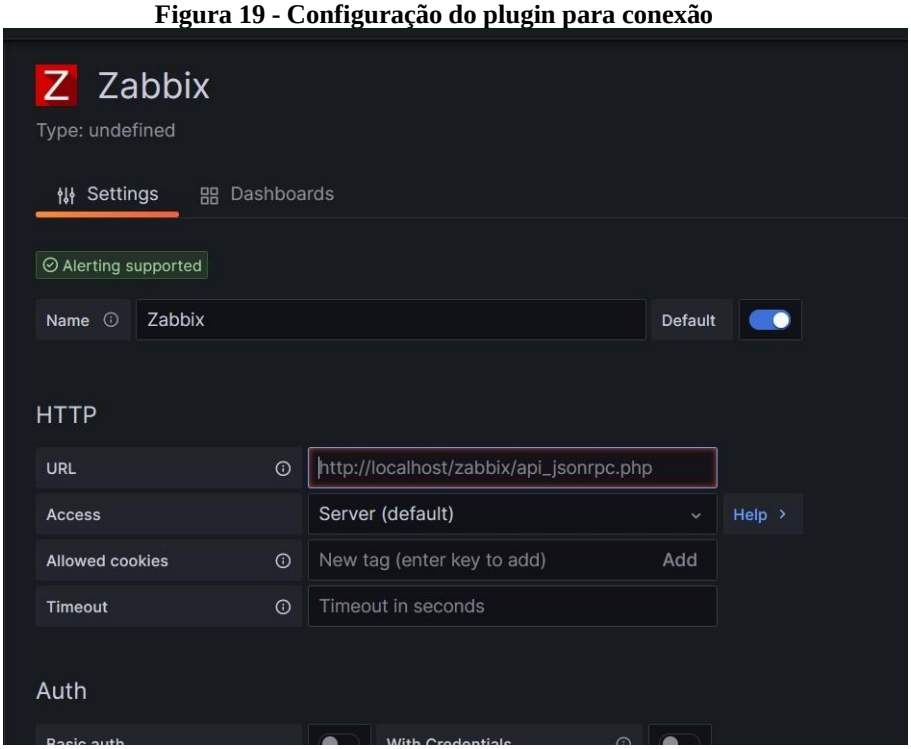
Fonte: Autores (2023)

Após a instalação do plugin, basta realizar a configuração da conexão com o banco de dados, para isso é preciso ir até o menu de conexões na aba de administração e selecionar o plugin para executar a configuração. A figura 19 demonstra a tela de configuração da conexão.

A imagem também apresenta um exemplo de como deve ser preenchido o URL para efetuar a integração entre os dois serviços. Em nosso caso o URL apresenta a seguinte estrutura: http://192.168.0.39/zabbix/api_jsonrpc.php.

Depois de realizada a inserção da URL de API, é necessário ainda criar um usuário e senha para que o grafana tenha acesso ao banco de dados. Um detalhe importante que deve ser feito para o funcionamento correto da conexão é a definição do nível de privilégios deste usuário, que precisa ser configurada como “Super admin role”.

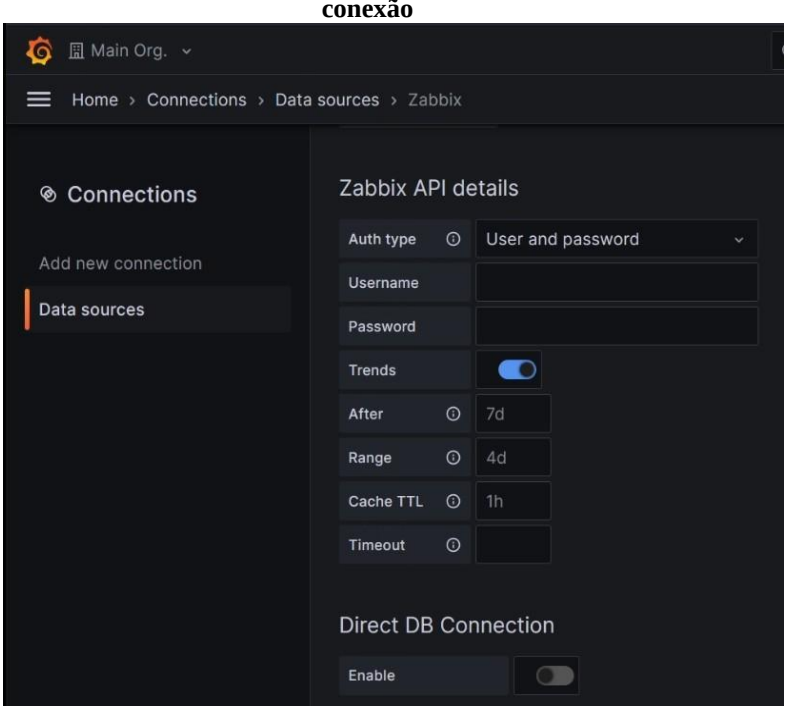
Figura 19 - Configuração do plugin para conexão



Fonte: Autores (2023)

Ainda na mesma tela, seguindo para o restante dos campos existentes, temos o local para preenchimento das credenciais de login. A figura 20 demonstra o local onde os campos estão para serem preenchidos.

Figura 20 - Campo de usuário e senha para conexão



Fonte: Autores (2023)

Caso todas as variáveis para configuração estejam corretas, a seguinte mensagem, demonstrada pela figura deve ser exibida, indicando que a configuração foi realizada com êxito.

Figura 21 - Conexão realizada com sucesso

Fonte: Autores (2023)

3. Criação e configuração de usuários

Para que um usuário possa visualizar a dashboard, criada por um administrador no zabbix, é necessário criar um perfil para este o utilizador. É importante que a criação de usuários seja feita tendo em mente qual a intenção de uso, no caso de um consumidor final, é interessante que o usuário não tenha permissões que autorizem modificações que possam alterar ou impedir o funcionamento correto da ferramenta.

No grafana, a criação de usuário é extremamente simples e intuitiva, basta navegar até o campo de administração, estando logado com uma conta de administrador, e selecionar a aba “Users”, onde há a opção de criar usuários. Basta preencher com as informações básicas de usuário, como nome, e-mail, nome de usuário e senha.

Após criado o usuário, deve ser definido o “papel” deste. Há três opções para papéisde usuário: Admin; Viewer e Editor. Em caso de um usuário final, o ideal é que o papel dele seja apenas de visualizador, pois é provável que pessoas sem conhecimento da ferramenta façam alterações indesejadas, comprometendo assim a integridade do monitoramento desenvolvido.

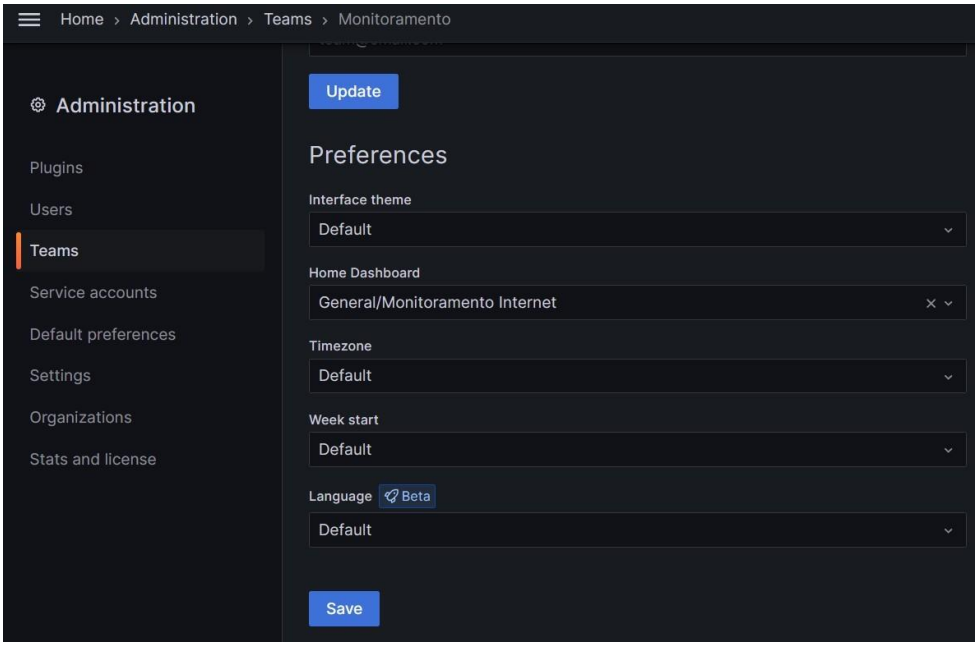
Para casos de administradores de T.I. de pequenas empresas ou outros negócios, que possuam conhecimento necessário para operar a ferramenta, é interessante fornecer o papel deeditor, ou até administrador, dependendo do grau de conhecimento.

Depois de criados os usuários que farão uso do monitoramento, devem ser

configurados os times aos quais estes usuários pertencerão. A criação de times é igualmente simples de ser executada. Na versão do grafana utilizada, a aba está localizada logo abaixo de usuários.

O intuito da criação de times neste caso, é definir uma nova página home para os usuários, fazendo com que a tela de monitoramento seja o primeiro item a ser visualizado quando realizado login no sistema. A figura 22 demonstra como ficou a definição de uma nova home para os participantes do time que foi criado. A configuração foi feita no campo "Home Dashboard".

Figura 22 - Configuração de uma nova página home



Fonte: Autores (2023)

4. Criação de painéis para monitoramento de ativos no grafana

No grafana, para exibir informações sobre um ativo monitorado, é preciso criar painéis e configurá-los da forma que apresente a melhor visualização a respeito do que está sendo exibido. Os painéis são responsáveis por coletar e exibir os dados capturados previamente pela ferramenta zabbix. A figura 23, por exemplo, mostra a estatística de falha do sinal. A informação é fornecida em porcentagem, de acordo com a taxa de perda de pacotes.

Figura 23 - Painel de exibição da falha de sinal

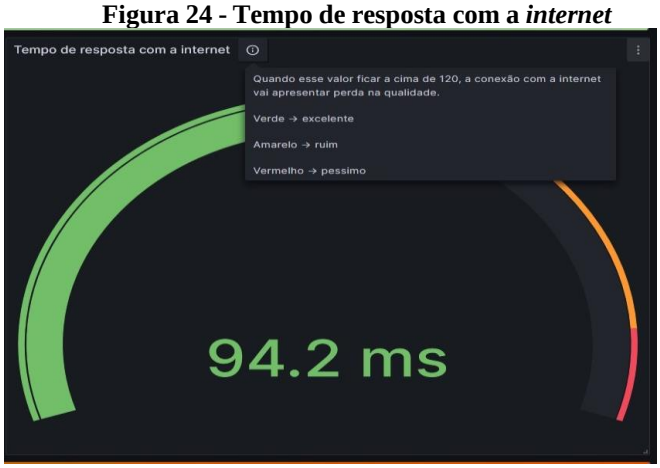
Fonte: Autores (2023)

Ainda tratando sobre a figura acima, podemos observar alguns pontos ressaltados na linha que percorre a parte inferior do painel. Os pontos demonstram momentos onde ocorreram perdas de pacotes. O gráfico está exibindo informações capturadas em um intervalo de 6 horas. Dessa forma, podemos assumir que ocorreram algumas perdas de pacote, que foram registrados pelo sistema de monitoramento neste período de tempo.

Outro painel criado para monitoramento foi o de tempo de resposta com a *internet*, que tem como missão mostrar a latência usando o DNS do google como parâmetro. A figura 24 demonstra a apresentação do painel. Este monitoramento pode variar de acordo com a provedora, pois algumas podem fornecer rotas de tráfego mais curtas, e consequentemente uma latência menor.

O contrário também é válido, pois é possível que a provedora de *internet* forneça uma conexão com rotas mais longas, e em decorrência deste fator, a latência será maior. No caso do ambiente monitorado, é comum que os valores de latência estejam situados entre 75 e 95 milissegundos.

Figura 24 - Tempo de resposta com a *internet*

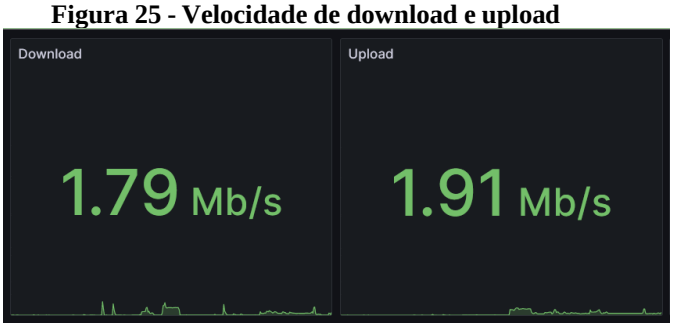


Fonte: Autores (2023)

O próximo painel a ser apresentado tem como objetivo demonstrar os valores de velocidade de download e upload atuais. Estes dados apresentam grande relevância para muitos usuários que buscam saber qual velocidade estão atingindo em relação a banda contratada. A figura 25 demonstra o painel em funcionamento.

Um fator relevante sobre esse monitoramento, é que com ele é possível detectar perdas na performance da conexão devido ao uso de *internet* estar próximo ao limite contratado. Com isso, o usuário pode alcançar conclusões que o levem a tomar melhor decisão, dentre as possibilidades temos, a diminuição do consumo de dados, ou uma melhoria do plano contratado para que supra a necessidade existente.

Figura 25 - Velocidade de download e upload



Fonte: Autores (2023)

Prosseguindo com a apresentação da dashboard, temos os painéis que exibem as informações de dados enviados e recebidos. Caso o roteador mikrotik seja desligado, as informações de quantidade de dados trafegados serão reiniciadas. O painel pode ser visualizado na figura abaixo.

Figura 26 - Dados consumidos

Fonte: Autores (2023)

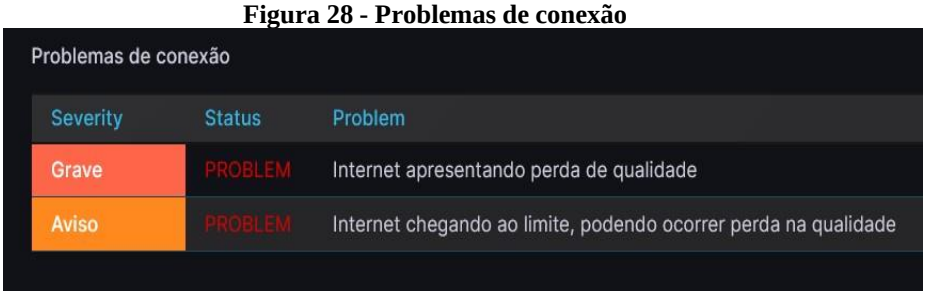
O penúltimo painel, apresentado na figura 27 tem uma função bem simples: Informar se há conexão com a *internet* sem exibir parâmetros, tais como latência e perda de pacotes. A tela exibe somente o texto “ONLINE” com fundo verde caso haja conexão com a *internet*, e “OFFLINE” com o fundo vermelho, caso esteja sem conexão com a *internet*.

Figura 27 - Status da conexão com a *internet*

Fonte: Autores (2023)

Para concluir a dashboard, temos o painel que exibirá os problemas de conexão detectados. O alerta para estes problemas deve estar previamente configurado no zabbix para que possam ser apresentados no grafana. As notificações criadas são 3: Sem *internet*; *Internet* chegando ao limite, podendo ocorrer perda na qualidade; e *Internet* apresentando perda de qualidade. Caso algum destes seja identificado, o painel exibirá. A figura 28 demonstra um exemplo de como funciona este recurso, caso algum problema esteja ocorrendo.

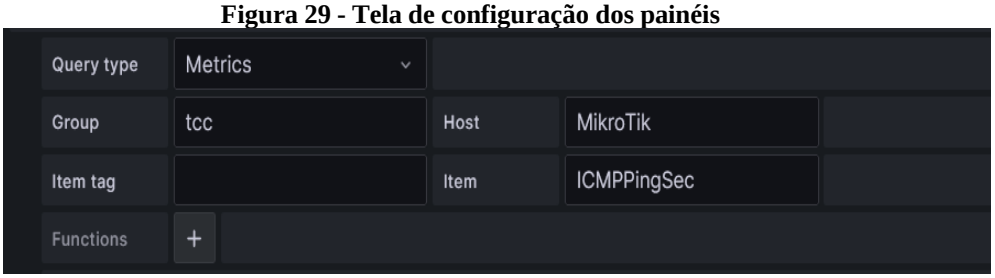
Figura 28 - Problemas de conexão



Fonte: Autores (2023)

Para que os painéis consigam capturar os dados advindos do banco de dados dozabbix, é necessário realizar a configuração do painel em questão. A figura 29 demonstra a tela de configuração dos painéis, onde são definidos os parâmetros de funcionamento ecaptura de dados.

Figura 29 - Tela de configuração dos painéis



Fonte: Autores (2023)

Os campos exibidos na figura acima são semelhantes para todos os painéis criados, neles devem ser preenchidos os tipos de query, que definem o aspecto da informação exibida, como métricas e problemas, o grupo do qual o host que será escolhido faz parte, o host, e o item que desejamos monitorar.

O campo item tag não foi utilizado, pois além de ser opcional, não cabe aqui o

uso deste filtro, pois não há tantos itens no grupo trabalhado para tornar necessário o uso deste recurso.

Com o conteúdo apresentado anteriormente no capítulo 4 e suas dependências, é encerrado aqui a apresentação dos alicerces que compõem os métodos, metodologias e artifícios utilizados para a elaboração do serviço de monitoramento de ativos rede que este documento se propusera a apresentar. Dessa forma, os conteúdos seguirão com a análise dos resultados proporcionados pela construção e implementação apresentada.

ANÁLISE E DISCUSSÃO DOS RESULTADOS

Finalizado o capítulo de material e métodos, a próxima etapa será a avaliação dos resultados obtidos com o sistema de monitoramento desenvolvido e apresentado por este documento acadêmico. Os capítulos subsequentes trarão elucidações acerca dos dados coletados durante o período de teste, demonstrando assim a eficiência do que foi desenvolvido, aplicado em um cenário real de uma pequena empresa.

RESULTADOS DA IMPLEMENTAÇÃO DE *HARDWARE*

O núcleo de funcionamento do monitoramento implementado é o *hardware* raspberry, que hospeda as ferramentas escolhidas, e o roteador MikroTik utilizado, dessa forma, estes serão os primeiros itens apresentados para início da análise e discussão dos resultados, pois compõe a infraestrutura que foi necessária para atingir os objetivos.

- **Apresentação do local e forma de instalação**

Como dito anteriormente, a implementação do projeto foi realizada em uma empresa de pequeno porte. O ecossistema de rede desta empresa será monitorado de forma geral. Como já referido previamente neste texto, para monitorar todos os dados trafegados, será conferido todo volume de tráfego que utilizar a porta 4 no roteador MikroTik para comunicação, e devido a forma como os dispositivos foram interligados, é imperativo que todos os dados passem por esta porta para alcançar o destino, como demonstrado na figura 2.

A rede da empresa apresenta uma quantidade considerável de equipamentos para

monitoria. A tabela 1 demonstra os principais dispositivos conectados à rede, apesar de que, devido a natureza de negócio da empresa, o número de dispositivos pode apresentar elevação neste valor em momentos específicos.

Tabela 1 - Dispositivos existentes na empresa

Tipo de dispositivo	Quantidade
Servidores	1
Desktops	5
Impressoras	1
Dispositivos sem fio(celulares, notebooks, câmeras e outros)	13
Switchs	2
Outros dispositivos com fio	2
Total	24

Fonte: Autores (2023)

Para o cenário da empresa a instalação foi feita conectando o roteador fornecido pela provedora, ao roteador MikroTik pela porta 4, depois conectando o switch principal da empresa na porta 3 do MikroTik. Para que não fossem conectados mais cabos, o raspberry foi vinculado por meio de conexão sem fio ao MikroTik, e como os dispositivos estão bem próximos, não houve problemas de estabilidade ou alta latência entre raspberry e MikroTik.

Durante o período de teste, foi desativado a função rede sem fio do roteador fornecido pela provedora, e deixado que somente o MikroTik ficasse responsável pela rede sem fio da empresa, dessa forma, todo o volume de tráfego foi afunilado para o MikroTik.

A empresa não possui um rack para alocar os recursos de rede, o que tornou a inclusão dos novos equipamentos um pouco mais trabalhosa, no entanto, utilizando o espaço disponível foi possível manter todos os equipamentos próximos, como demonstra a figura abaixo.

Figura 30 - Equipamentos em funcionamento no local

Fonte: Autores (2023)

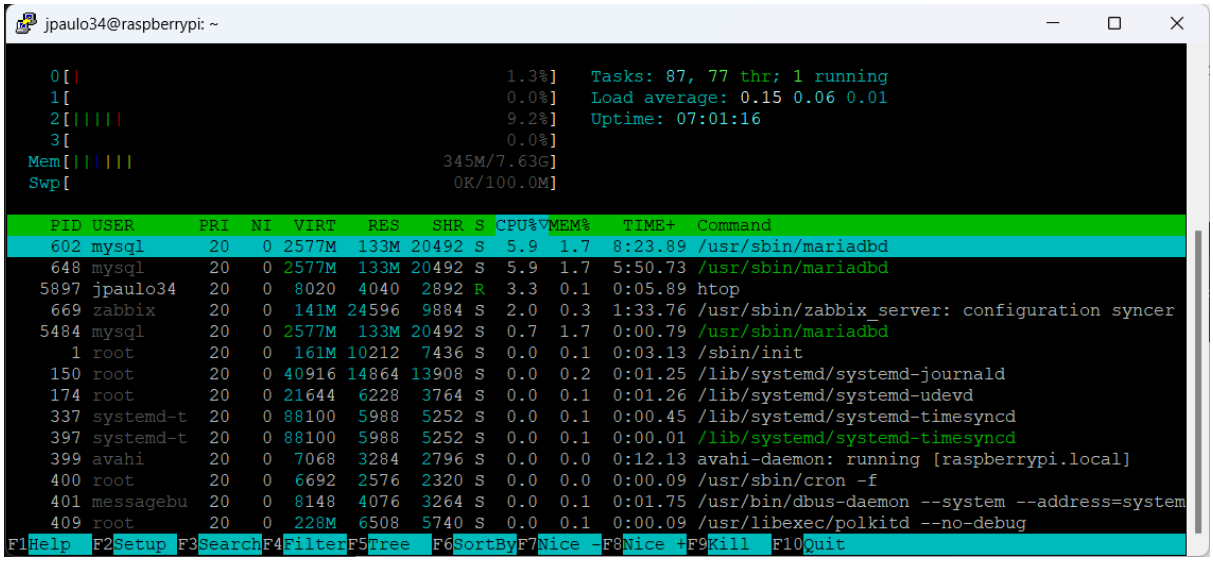
- **Estatísticas de desempenho do *hardware* utilizado**

Uma das preocupações existentes era quanto ao desempenho do raspberry quando o monitoramento estivesse ativo. Como são feitas consultas ao banco de dados de forma constante, houve receio de que talvez o *hardware* não fosse capaz de atender a todas as requisições recebidas, gerando atrasos, informações inconsistentes, travamentos constantemente ou mesmo a completa interrupção do funcionamento, sendo necessário uma reinicialização forçada.

Além da capacidade de processamento, também foi alvo de preocupações a capacidade de multitarefas do raspberry, por conta da hospedagem de duas ferramentas que operam de forma simultânea.

No entanto, apesar das preocupações, durante o período de teste os 8GB de memória RAM disponíveis provaram-se mais que suficientes, em conjunto com um sistema operacional baseado em debian, que apresentou baixo uso de recursos em segundo plano. Não foram recorrentes os momentos em que o monitor de recursos do sistema operacional apresentou consumo de RAM acima dos 800MB. O resultado também foi positivo para o uso de CPU, que comumente não ultrapassa os 40% de utilização, mesmo com todas as consultas. A figura 31 demonstra o consumo de recursos de *hardware* durante o funcionamento de 7 horas.

Figura 31 - Uso de de recursos computacionais durante as atividades de monitoramento



Fonte: Autores (2023)

Os resultados demonstraram que no quesito capacidade de processamento, o *hardware* estava atendendo a demanda com satisfação apresentava margem razoável para um uso de recursos de CPU mais intensos, porém em quesito de memória RAM, boa parte foi subutilizada, o que leva a duas possibilidades principais: Utilizar um *hardware* com menor capacidade de memória RAM, e igual desempenho de CPU, ou implementar outros recursos ou *softwares* de monitoramento.

A vantagem de utilizar um *hardware* com 4GB de memória, que contém uma das versões disponíveis do raspberry 4 seria redução de custos, e ainda assim, haveria boa margem para momentos em que fosse exigido maior uso de RAM.

RESULTADOS OBTIDOS DOS RECURSOS DE MONITORAMENTO

Nos subcapítulos a seguir serão apresentados os resultados obtidos com o sistema de monitoramento aplicado, e sua eficiência para com a missão proposta por este trabalho de conclusão de curso, bem como a visualização dos resultados e a influência destes para a comprovação do funcionamento, por meio de registros visuais e análises.

- **Dashboard criada no zabbix**

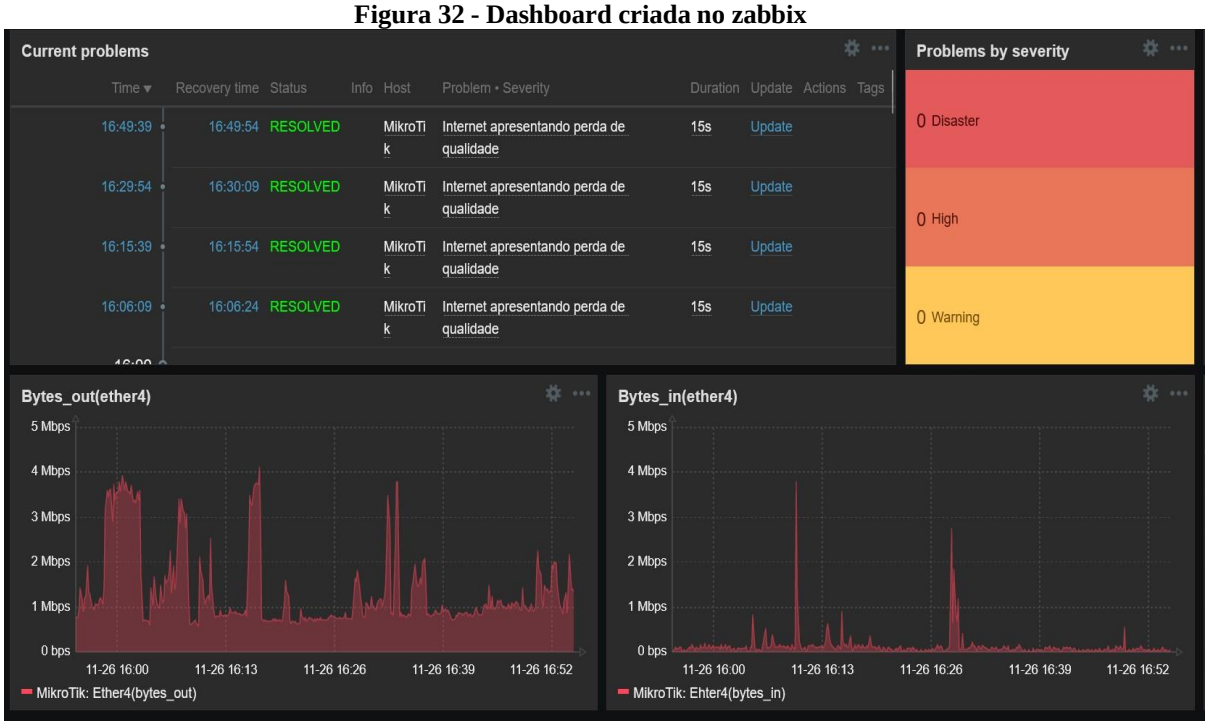
Para visualização das informações capturadas, foi criado uma dashboard no zabbix, que permitiu a análise do comportamento dos dados de acordo com a configuração realizada. Com isso foi possível aprimorar a forma de exibição destes dados, corrigindo problemascomo o fato da captura de alguns parâmetros não registrar a informação na unidade desejada.

Apesar de permitir a visualização das informações, a dashboard no zabbix foi criada apenas para testes de captura de dados, pois os painéis não são muito intuitivos, e apresentam uma interface que não é amigável a um usuário leigo ou com pouco conhecimento técnico.

É evidente a possibilidade de alteração de alguns parâmetros de exibição dos gráficos, no entanto, a variedade de opções é reduzida, não permitindo grandes alterações e por consequência, mantendo o aspecto original, não muito convidativo da ferramenta. A figura 32 apresenta alguns itens configurados na dashboard utilizada para testes no zabbix.

De certa forma a interface apresenta mais informações, como exibição de eventos em um intervalo de tempo maior, porém o excesso de informações pode não ser bem-vindo em um cenário onde o interesse é manter a simplicidade. Vale lembrar que por se tratar de um modo de testes dos parâmetros, nem todos itens capturados estão sendo exibidos na figura abaixo.

Figura 32 - Dashboard criada no zabbix



Fonte: Autores (2023)

- **Dashboard criada no grafana**

Em contraponto a dashobard do zabbix, o grafana oferece maiores recursos para modificar a visualização dos painéis criados, tornando mais intuitivo a visualização de informações como latência, perda de pacotes, velocidade de upload e download, e dados trafegados. As figuras 33 e 34 apresentam a visualização completa da dashboard criada no grafana.

Figura 33 - Parte superior da dashboard no grafana

Fonte: Autores (2023)

Figura 34 - Parte inferior da dashboard no grafana

Fonte: Autores (2023)

- **Dados registrados pela dashboard**

Apresentado então a dashboard final no capítulo anterior, agora discutiremos sobre os registros realizados pelo sistema de monitoramento e a relevância dessas informações. Também será demonstrado o funcionamento da dashboard, e de que forma ela exibe os dados de acordo com o que está ocorrendo na rede, por meio de alertas e variações no modo de exibição da interface.

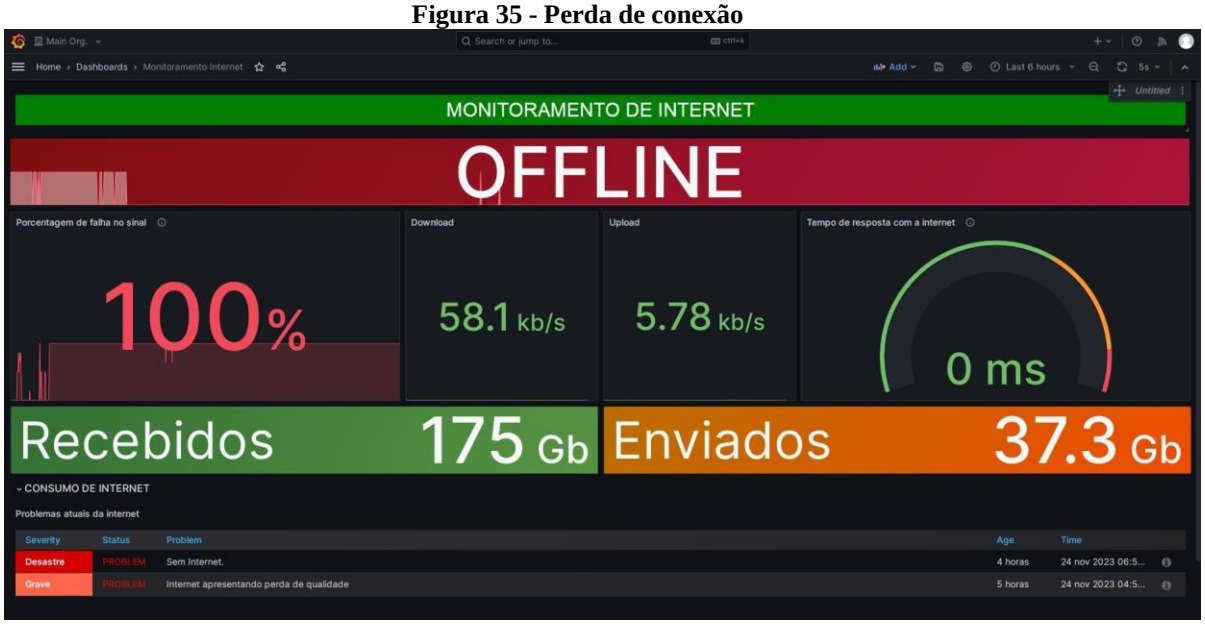
- **Perda de conexão com a *internet***

A figura 35 demonstra um cenário real, onde a empresa em que o monitoramento

está capturando dados, sofreu uma perda total da conexão da rede local com a *internet*, ou seja, o pior cenário possível. Nesse caso os painéis de porcentagem de falha do sinal e status da conexão mudarão as informações exibidas de acordo com essa situação, onde a mensagem de "ONLINE" será substituída por "OFFLINE" e trocará o fundo verde por um fundo vermelho, para auxiliar no entendimento visual de que há um problema.

O painel de porcentagem de falha do sinal indicará 100% de perda de pacote e também ficará vermelho. Ainda neste cenário, o painel de problemas exibirá notificações sobre o que está ocorrendo, o momento de início do evento, e a quanto tempo está ocorrendo, bem como o nome do problema e o nível de severidade.

Figura 35 - Perda de conexão



Fonte: Autores (2023)

Ainda sobre a figura 35, pode-se notar que o gráfico de tempo de resposta está exibindo 0 ms, isso ocorre porque como a rede local está sem acesso à *internet*, não possível verificar o tempo de resposta com o DNS do google, porém, apresentar 0 ms não representa algo bom, pelo contrário, indica a falta de conexão.

- **Saturação de banda**

Outro cenário de comum ocorrência é a saturação da banda contratada, que ocorre quando os dispositivos na rede estão usando todo o espaço de transmissão disponível. Quando uma situação do tipo ocorre, é possível notar também um aumento de latência, e falha na transmissão de pacotes. A figura 36 demonstra como reage o

monitoramento em um eventodestes.

Figura 36 - Saturação de banda

Fonte: Autores (2023)

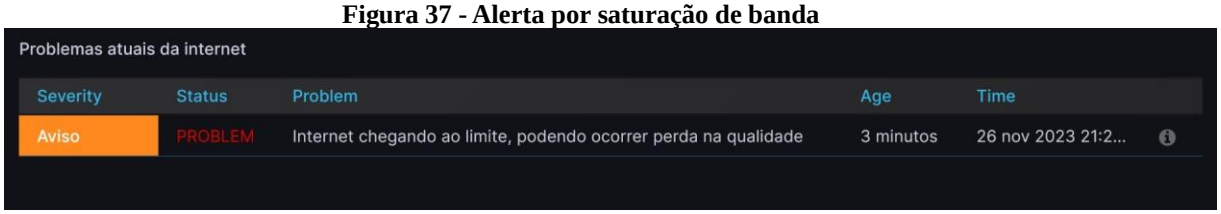
Quando a velocidade de download ultrapassa 80% do que está disponível, o gráfico muda para a cor amarela, já quando os valores ultrapassam 90%, o gráfico se torna vermelho, indicando que está próximo do limite. O mesmo comportamento ocorre no gráfico de tempo de resposta.

Este evento de saturação pode ocorrer quando o espaço de transmissão de download, ou de upload atinge o limite, e dependerá de fatores como equipamentos presentes na rede, e o plano de *internet* contratado. No caso da empresa onde está sendo monitorado, o plano de *internet* contratado é assimétrico, e fornece 100 megabits de download e 60 megabitsde upload.

Outro sintoma que pode ocorrer quando a banda está em saturação, é a perda de pacotes. Isso não necessariamente ocorrerá todas as vezes em que a banda for saturada, mas é uma possibilidade, pois, ao chegar ao limite de transmissão de pacotes, os novos pacotes requisitados não serão atendidos por falta de espaço de transmissão, logo, serão descartados, oque acarretará a perda de pacotes.

A figura 37 demonstra o painel de problemas de conexão exibindo o alerta devido a banda ter sido saturada, e informa que pode ocorrer perda de qualidade. Desta forma, encerra-se a apresentação dos resultados.

Figura 37 - Alerta por saturação de banda



Fonte: Autores (2023)

CONSIDERAÇÕES FINAIS

O presente capítulo marca o desfecho do desenvolvimento da pesquisa proposta, e conclui a implementação e análise crítica da pesquisa de monitoramento de rede, empregando o *hardware* Raspberry Pi como servidor e as robustas ferramentas Grafana e Zabbix para a visualização e análise dos dados. Ao longo dos capítulos anteriores, exploramos os fundamentos teóricos, delineamos a metodologia empregada e apresentamos os resultados obtidos. Desta forma, serão apresentadas a seguir, as conclusões obtidas, descobertas, e suas implicações, bem como possíveis melhorias.

Após implementado o monitoramento, foi possível realizar o acompanhamento das informações de tráfego atuais da rede, demonstrando estatísticas de consumo de dados geral, capacidade de download e upload utilizadas, latência, e falhas de conexão. Além disso, também foi possível exibir problemas detectados na rede para alertar o usuário sobre falhas que possam impedir a utilização de recursos que necessitem de *internet*, ou mesmo apenas reduzem a qualidade da navegação, comprometendo a experiência do usuário e também reduzindo sua eficiência em serviços e atividades que dependam de uma conexão estável.

Tendo em mente as informações apresentadas anteriormente, é possível inferir que os objetivos elaborados foram atingidos com sucesso, e essa asserção é válidada quando na pesquisa foi utilizado um *hardware* dedicado para hospedar as ferramentas utilizadas, que no caso foi o Raspberry Pi, hospedeiro do zabbix, que por sua vez realiza a coleta de dados, para transmiti-los ao grafana, também hospedado no raspberry, para então exibir os dados adquiridos em uma interface *web*, acessível pelo navegador e aplicativo mobile do grafana.

Dessa forma, com o objetivo do estudo atingido, resta apresentar as possíveis melhorias futuras, tais como a implementação de um painel para exibição da quantidade de dispositivos conectados na rede. Além da anterior, também há a possibilidade da criação de um gráfico para a demonstração da porcentagem do tempo em que a conexão com a *internet* esteve disponível durante o período de um mês. Outra adição valorosa seria a inclusão do downdetector para apresentar aos usuários quais dos serviços mais acessados estão fora do ar, ou com algum problema, diretamente na interface do grafana.

Como último ponto a citar para melhorias, temos a possibilidade de utilizar um único dispositivo gerenciador. Isso eliminaria o MikroTik e o raspberry, e levaria suas

funções para um SBC (Single Board Computer) que utilizasse também a arquitetura ARM para manter o baixo de consumo de energia, e também viabilizar a instalação das ferramentas de *software* utilizadas em um único local, que reduziria a dificuldade de instalação por precisar de menos pontos de energia.

Finalizando este documento acadêmico, concluímos que o estudo apresentou resultados satisfatórios, e até mesmo superou em alguns aspectos a proposta inicial, demonstrando excelente potencial para monitoramento de *link*s de *internet*.

REFERÊNCIAS BIBLIOGRÁFICAS

COMER, D. E. **INTERLIGAÇÃO DE REDES COM TCP/IP PRINCÍPIOS, PROTOCOLOS E ARQUITETURA**. 6. ed. Porto Alegre: Elsevier Editora Ltda, 2016.

FEW, S. **INFORMATION DASHBOARD DESIGN**. Italy: O'Reilly, 2006.

FOROUZAN, B. A. **COMUNICAÇÃO DE DADOS E REDES DE COMPUTADORES**. São Paulo: AMGH Editora LTDA, 2010.

HALFACREE, G. **THE OFFICIAL RASPBERRY PI BEGINNER'S GUIDE HOW TO USE YOUR NEW COMPUTER**. Cambridge: Raspberry Pi Trading Ltd, 2020.

HERTZOG, R.; MAS, R. **O MANUAL DO(A) ADMINISTRADOR(A) DEBIAN**. 1. ed. [s.l.] Freexian SARL, 2020.

IBM. **CONCEITOS DE REDE E COMUNICAÇÃO**. Disponível em: <https://www.ibm.com/docs/pt-br/aix/7.3?topic=management-network-communication-concepts>. Acesso em: 28 set. 2023.

KUROSE, J. F.; ROSS, K. W. **COMPUTER NETWORKING A TOP-DOWN APPROACH**. 7. ed. England: Pearson Education Limited, 2016.

MONK, S. **RASPBERRY PI COOKBOOK**. Sebastopol: O'Reilly Media, Inc., 2023.

SAROLAHTI, P. **CONGESTION CONTROL IN LINUX TCP**. Disponível em: <https://www.usenix.org/legacy/event/usenix02/tech/freenix/full_papers/sarolahti/sarolahti_html/>. Acesso em: 16 nov. 2023.

SOUSA, L. B. DE. **TCP/IP E CONECTIVIDADE EM REDES: GUIA PRÁTICO**. 5. ed. São Paulo: Érica LTDA, 2009.

STALLINGS, W. **DATA AND COMPUTER COMMUNICATIONS**. 10. ed. Boston: Pearson Education, Inc., 2013.

STALLINGS, W. **CRIPTOGRAFIA E SEGURANÇA DE REDES: PRINCÍPIOS E PRÁTICAS**. 6. ed. São Paulo: Pearson Education do Brasil Ltda, 2014.

TANENBAUM, A. S.; WETHERALL, D. **REDES DE COMPUTADORES**. 5. ed. São Paulo: Pearson, 2013.

TORRES, G. **REDES DE COMPUTADORES**. 2. ed. Rio de Janeiro: Clube do *Hardware*, 2004.