Implementação do Monitoramento de Redes com Zabbix

Débora Cristina Santos de Brito[1], José Vigno Moura Sousa[1,2]

[1]Universidade Estadual do Piauí (UESPI)
Piripiri, Piauí
Brasil

[2]Laboratório de Engenharia de Software (LES)
Piripiri, Piauí
Brasil

deboracbrito@aluno.uespi.br, josevigno@prp.uespi.br

Abstract. *Zabbix is a monitoring tool used to maintain secure and stable networks. Its versatility allows it to be applied to various environments, including companies, businesses and academic institutions. This study aimed to apply Zabbix to monitor two campuses of the State University of Piauí, located in Teresina and Piripiri. Real-time data, such as bandwidth usage, server load and service availability, was collected and then stored in a MariaDB database. Using Grafana Dashboards allowed network administrators to monitor the infrastructure, identifying problems and taking proactive measures to ensure the smooth functioning of the network.*

Resumo. *Zabbix é uma ferramenta de monitoramento usada para manter redes seguras e estáveis. Sua versatilidade permite aplicação para vários ambientes, incluindo empresas, comércios e instituições acadêmicas. Este estudo, teve como objetivo aplicar o Zabbix para monitorar dois campus da Universidade Estadual do Piauí, localizada em Teresina e Piripiri. Foram coletados dados em tempo real, como o uso de largura de banda, carga do servidor e disponibilidade de serviços, e em seguida armazenados em um banco de dados MariaDB. A utilização de Dashboards do Grafana permitiu aos administradores de redes monitorar a infraestrutura, identificando problemas e tomando medidas proativas para garantir o bom funcionamento da rede.*

1. Introdução

O surgimento do computador mecânico no século XIX, foi uma grande inovação para época. Os estudos na área da tecnologia aumentou e culminou na criação da internet, uma rede onde os dispositivos estão interconectados, facilitando o compartilhamento de informações em uma escala global. Essas descobertas mudaram a forma de se viver e trabalhar, permitindo uma maior democratização do conhecimento e melhorias em diversas áreas, como: o comércio, a ciência e tecnologia.

Devido ao crescimento exponencial da quantidade de redes em comunicação, a complexidade aumentou significativamente, destacando a necessidade de maior controle e segurança. Como resposta a essa demanda, surgiu a profissão de administrador de rede. Como aponta [Comer 2007]: "um administrador trabalha para

detectar e corrigir problemas que tornam a comunicação ineficiente ou impossível e eliminar as condições que produzirão o problema novamente. Porque falhas de hardware e de software podem causar problemas, mas, um administrador de rede deve monitorá-las".

Além do mais, o monitoramento é uma prática fundamental para acompanhar o desempenho das atividades em uma rede de computadores, garantindo seu funcionamento adequado. Isso envolve a coleta de informações em tempo real sobre dispositivos, servidores, aplicativos e outros componentes de infraestrutura de rede. Para isso, os administradores de redes podem se valer de ferramentas específicas como Nagios, Zenoss e o Zabbix, mencionadas no artigo de [Mohr 2012] suas vantagens e desvantagens distintas.

O Nagios é uma das ferramentas mais antigas e consolidadas no mercado de monitoramento. Isso significa que ele oferece uma ampla gama de *plugins* e uma comunidade ativa de desenvolvedores. No entanto, sua interface de usuário pode parecer desatualizada em comparação com ferramentas mais recentes. A configuração inicial demanda um trabalho manual considerável, o que pode ser um obstáculo para iniciantes.

Por outro lado, o Zenoss oferece uma abordagem de monitoramento unificada que abrange infraestrutura, aplicativos e redes em uma única plataforma. Isso simplifica a gestão, uma vez que os responsáveis podem obter uma visão completa do ambiente de Tecnologia da Informação (TI) em um só lugar. No entanto, sua configuração pode ser complexa, envolvendo a definição de modelos de dispositivos e serviços.

O Zabbix se destaca por sua interface amigável, coleta de dados avançada, notificações configuráveis e suporte a diversos dispositivos. A configuração inicial pode ser desafiadora para iniciantes, demandando tempo para se familiarizar com a ferramenta. No entanto, uma vez configurado corretamente, o Zabbix oferece um poderoso conjunto de recursos de monitoramento que o tornam uma escolha popular entre os administradores de redes.

Sem um monitoramento, as empresas estão sujeitas a falhas, perda de dados e, consequentemente, a prejuízos financeiros. De acordo com [Fotios 2021], os vazamentos de dados no Brasil aumentaram impressionantes 493%. Além disso, um estudo da [Shandwick 2022] revelou que o tempo médio para detectar e conter incidentes de segurança em redes é significativamente alto no Brasil, atingindo 347 dias. O custo médio varia: empresas que levam mais de 200 dias para resolver o problema enfrentam um custo médio de R$ 7,71 milhões, enquanto aquelas que resolvem antes desembolsam em média R$ 5,19 milhões.

Quando um rede está vulnerável existem vários tipos de ameaças, como ataques de hackers, onde pessoas ou organizações secretas invadem sistemas e roubar informações confidenciais. Em empresas e universidades, essa exposição é preocupante, por terem dados sensíveis, como informações bancárias e notas acadêmicas, podem ser acessados e até alterados por indivíduos não autorizados. Além de tudo, a rede pode ser comprometida por vírus que causam danos aos sistemas, prejudicando o funcionamento da organização como um todo.

Conforme destacado anteriormente, ter uma rede desprotegida é preocupante, isso denota a importância do monitoramento e a necessidade de utilizar ferramentas adequadas. Nesse contexto, o objetivo deste trabalho foi implantar o Zabbix como ferramenta de monitoramento de redes na Universidade Estadual do Piauí (UESPI), facilitando a detecção problemas e encontrando soluções mais rápidas, evitando que a estrutura fique indisponível por determinado período. Desse modo, contribuiu para melhorar a qualidade do serviço de rede da UESPI, além de promover a disseminação de conhecimento sobre as tecnologias de monitoramento de redes para a comunidade acadêmica.

2. Trabalhos Relacionados

Os computadores deixaram de ser maquinas isoladas e passaram a ser uma rede interconectada. Essa expansão, tanto de dispositivos e equipamentos de rede, faz com que os serviços de tecnologia da informação que atuam nessas organizações que dependem da rede para seu funcionamento, tenham um nível de disponibilidade maior, tornando evidente a necessidade de monitoramento [SILVA 2015]. No trabalho de [Mohr 2012], é feito um comparativo de três ferramentas de monitoramento de redes, Zabbix, Nagios e Zenoss, e chegou à conclusão de que o Zabbix é o mais completo, por ter uma boa interface e poder computacional.

No estudo conduzido por [Paula et al. 2016], implementou o Zabbix no Instituto Federal Goiano Campus Morrinhos a fim de garantir a disponibilidade e confiabilidade dos serviços de TI oferecidos pelo campus. Utilizou os protocolos SNMP e ICMP, para coletar informações de equipamentos como câmeras de segurança, telefones VoIP, antenas sem fio nanostations. Ademais, usou 16 *templates*, sendo alguns padrões da própria ferramenta. Para detectar problemas, manuseou o envio de mensagens através do aplicativo whatsapp e e-mail. Por fim, disponibilizou a geração de gráficos e relatórios que ajudaram na análise de desempenho e gerenciamento de capacidade da rede.

No trabalho descrito por [dos Santos et al. 2020], foi implementado um monitoramento proativo usando Zabbix, na Universidade Federal de Mato Grosso (UFMT). Empregando a tecnologia de container, para isso fez o uso da ferramenta Docker. O primeiro passo foi fazer uma lista dos agentes ativos com seus referentes modelos, marcas e endereços IP's. Também se utilizou os protocolos SNMP e ICMP para cadastrar os equipamentos da lista feita anteriormente, obtendo assim os dados e status dos dispositivos em tempo real, como taxa de tráfego de cada interface, o uso da memória RAM e da *Central Processing Unit*(CPU). Por fim, possibilitou a diminuição do tempo de atendimento ao desenvolver scripts em Pyhton para o enviar mensagens de notificação aos administradores de rede pelo Telegram, sobre qualquer problema nos equipamentos.

Em [Bueno 2022], descreve o uso da combinação do Zabbix e do Grafana, visando simplificar o monitoramento de dispositivos em uma rede doméstica. O Grafana oferece gráficos para a análise de informações, permitindo a personalização das informações a serem exibidas e o intervalo de tempo desejado. Destaca também a importância do monitoramento contínuo, especialmente em ambientes empresariais. Por último, é importante destacar que o Zabbix se mostrou muito versátil nos *host*

monitorados. Após ser instalado, o Zabbix demonstra sua adaptabilidade e facilidade de configuração, eliminando a necessidade de ajustes adicionais nas estações onde está implantado. Todas as demais configurações podem ser realizadas de forma direta no servidor do Zabbix.

Com base nas problemáticas de uma rede desprotegida pode acarretar, identificou-se a necessidade de monitorar um servidor da UESPI usando a ferramenta Zabbix. Para reforçar a segurança, implementou-se o uso da ferramenta de e-mail para enviar alertas. Além disso, foram empregados os protocolos SNMP e ICMP que coletam informações dos equipamentos, incluindo dispositivos Mikrotik. Realizou-se o aprimoramento da visualização dos dados coletados pelo Zabbix utilizado o Grafana como uma ferramenta para gerar gráficos, que foram disponibilizados para a equipe de rede.

3. Proposta do Trabalho

O objetivo deste trabalho foi implementar o monitoramento de rede, em roteadores, serviços web, máquina virtual e entre outros; por meio da ferramenta chamada Zabbix. Além disso, ocorreu a configuração para enviar mensagens de alertas para a equipe de TI utilizado o e-mail, tanto para problemas críticos quanto não críticos. O Grafana também se integrou ao sistema, para melhorar a visualização dos dados. A ênfase está em garantir a disponibilidade e estabilidade da rede na UESPI nos campus Poeta Torquato Neto (Teresina - PI) e campus Prof. Antônio Giovani Alves de Sousa (Piripiri-PI).

3.1. Materiais e Métodos

Para alcançar os objetivos estabelecidos, foi necessária a configuração de containers, uma forma de virtualização mais leve que permite a execução de aplicações isoladas no mesmo sistema operacional do hospedeiro. Diferente das máquinas virtuais, que emulam sistemas completos. Na UESPI de Piripiri, o sistema operacional utilizado é o Ubuntu 20.04.6 LTS, enquanto na UESPI de Teresina é o Debian GNU/Linux 11 (bullseye).

Segundo [SIA 2024a] e mostrado na Tabela 1, o monitoramento pode ser classificado com base na quantidade de métricas, que varia de 1.000 em instalações pequenas a 1.000.000 em ambientes de grande escala. Conforme [SIA 2024b] e na Tabela 2, a classificação considera a quantidade de *hosts*, indo de 100 para instalações pequenas a mais de 10.000 em grandes. Após identificar o tamanho da instalação, existem padrões de configuração de hardware a serem seguidos, como CPU e memória. No entanto, devido ao baixo número de *hosts* deste trabalho, foi utilizado um total de 2,0 GiB de memória em ambos os casos.

Tabela 1. Exemplos de configuração de hardware Zabbix versão 6

Tamanho da instalação	Métricas monitoradas	CPU	Memória (GiB)
Pequeno	1 000	2	8
Médio	10 000	4	16
Grande	100 000	16	64
Muito grande	1 000 000	32	96

Tabela 2. Exemplos de configuração de hardware Zabbix versão 5

Nome	Plataforma	CPU/Memória	Hosts Monitorados
Pequeno	CentOS	Dispositivo virtual	100
Médio	CentOS	2 núcleos de CPU/2GB	500
Grande	Red Hat Enterprise Linux	4 núcleos de CPU/8 GB	>1000
Muito grande	Red Hat Enterprise Linux	8 núcleos de CPU/16 GB	>10.000

Após a configuração dos containers, o Zabbix foi inicialmente instalado e configurado no container de Piripiri, utilizando a versão 5.0.36, sendo esta a primeira a passar pelo processo de teste. Posteriormente, no container de Teresina, foi instalada a versão 6.0.21 do Zabbix. Ademais, o banco de dados MariaDB, nas versões 10.3.39 em Piripiri e 10.5.21 em Teresina , foi configurado para armazenar os dados coletados, garantindo a segurança na manipulação dessas informações.

Antes de começar o próprio monitoramento, realizou-se uma avaliação como os administradores de rede para identificar quase ativos eram primordiais para manter um controle constante e seus protocolos de internet (IPs). Ademais, uma configuração no dispositivo e no container Zabbix caso seja necessário, um exemplo disso é quando o monitoramento é feito por meio do SNMP, que precisa ser instalado e configurado em ambos.

Com essas etapas concluídas, o monitoramento foi iniciado. A Figura 1 apresenta como esse processo ocorre: no centro da imagem, está representado o servidor do Zabbix, onde toda a aplicação é executada. À direita, estão os ativos a serem monitorados, utilizando agentes, protocolos SNMP ou sem agentes. À esquerda, encontra-se a interface web, através da qual os ativos são monitorados e os dados coletados são armazenados no banco de dados.

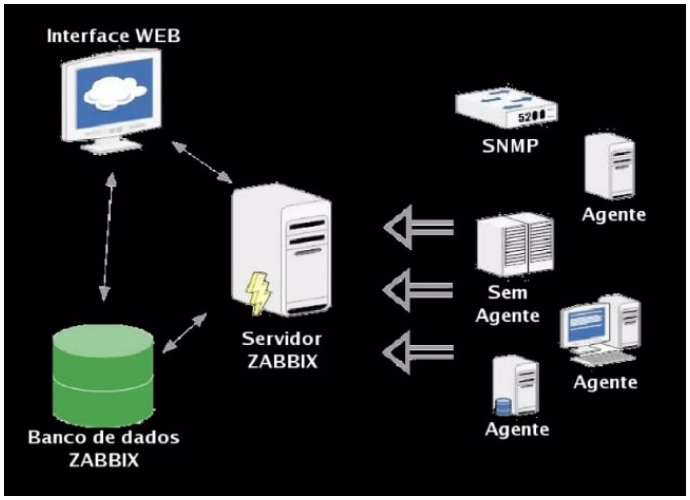

Figura 1. Funcionamento do Servidor Zabbix
Fonte: [Bauermann 2010]

Primeiro realizou-se a criação um grupo de *host* para cada tipo de monitoramento, por exemplo o grupo "proxmox"a qual máquinas virtual estão participando. Em seguida, ocorreu a configuração de todos, incluindo servidores de rede, web e dispositivos de rede. Cada um foi adicionado no Zabbix como um *host* individual, identificado por seu nome, endereço IP e template correspondente, podendo ter mais de um no grupo. Na Figura 2, estão os *hosts* do Campus de Teresina, e na Figura 3, os de Piripiri.

Nome ▲	Itens	Triggers	Gráficos
DNS Primario	Itens 67	Triggers 26	Gráficos 13
DNS Secundario	Itens 42	Triggers 14	Gráficos 8
Entrada da DTIC	Itens	Triggers	Gráficos
MikroTik01	Itens 1311	Triggers 610	Gráficos 65
nucepe web	Itens 68	Triggers 27	Gráficos 14
Proxy Reverso 1	Itens 71	Triggers 30	Gráficos 14
Proxy Reverso 2	Itens 68	Triggers 27	Gráficos 14
Site da Editora	Itens 68	Triggers 27	Gráficos 14
Site da UESPI	Itens 68	Triggers 27	Gráficos 14
Zabbix server	Itens 125	Triggers 69	Gráficos 25

Figura 2. Hosts do Campus Teresina
Fonte: Autoria própria

Nome
Zabbix server
BD
Zabbix SNMP
MikroTik
114 Deb - Zabbix
Servidor_teste_1
proxy-reverso
Psono
Grafana-NPD
BancoDeDados
Node-Red
Mosquitto
LuanDeploy

Figura 3. Hosts do Campus Piripiri
Fonte: Autoria própria

Em seguida, utilizou-se alguns *templates* pré-definidos pela ferramenta Zabbix,

na Tabela 3 enumera todos eles, são responsáveis por fornecer as configurações e funcionalidades necessárias para cada tipo de monitoramento. O *template* 1 foi projetado para coletar informações específicas de sistemas operacionais Linux usando o agente Zabbix. Ele possuí métricas como CPU, memória, espaço em disco, processos, entre outros. É essencial para monitorar o desempenho e a saúde de servidores Linux.

Do mesmo modo, o *template* 2 é focado em monitorar a saúde do próprio servidor Zabbix. Ele inclui métricas como a carga do servidor, o status do banco de dados, a conectividade com os agentes, entre outros. Isso garante que o servidor esteja operando eficientemente.

O *template* 3 serve para monitorar mikrotik por meio do SNMP (Simple Network Management Protocol). Ele inclui métricas como uso de largura de banda, temperatura, status da interface, entre outros.

Além disso, foi utilizado o *template* 4, para monitorar dispositivos de rede ou servidores usando o protocolo ICMP Ping. Ele permite verificar se um dispositivo está online e respondendo a solicitações de *ping*. Pode incluir métricas como tempo de resposta, perda de pacotes, e outros parâmetros relacionados à conectividade.

Tabela 3. Templates utilizados

ID	Nome do Template
1	Template OS Linux by Zabbix agent
2	Templates Zabbix server health
3	Template Mikrotik by SNMP
4	Template Module ICMP Ping

Em cada *host* existe uma funcionalidade chamada WEB que permite verificar o status das URLs e determinar se o site está ativo ou inativo com base nos códigos de status retornados. Como é visto, na figura 4 onde 200 é o valor de ativo . Esses cenários web, foram utilizados para testar o funcionamento dos sites da instituição. Na figura 5 mostra o gráfico da velocidade de download.

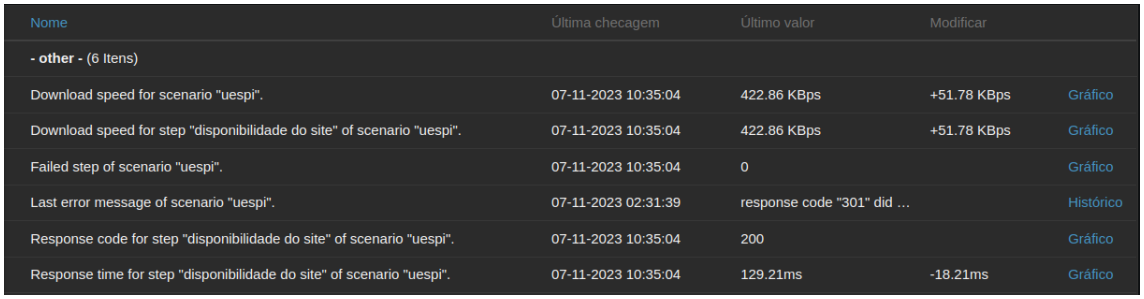

Figura 4. Web parâmetros
Autoria própria

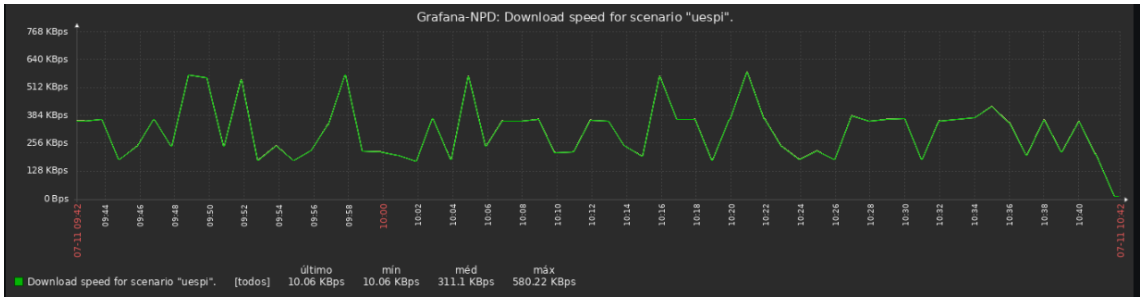

Figura 5. Web Gráfico
Autoria própria

Para cada *host* configurado, identificou-se itens relevantes, de acordo com os recursos específicos de cada um. Por exemplo, para o *template Linux by Zabbix agent* existe um item chamado *Available memory* que é fundamental para o monitoramento, pois verifica qual é a memória disponível da máquina. A partir daí, *triggers* também passaram-se a ser definidas com base nos valores monitorados, que acionam alertas caso os valores padrões de rede sejam ultrapassados.

Como afirma [SIA 2024c] "Uma expressão de trigger permite definir um limite aceitável de dados. Logo, quando o dado recebido fugir do limite aceitável a trigger será acionada, mudando seu estado para INCIDENTE". Elas são essenciais para identificar situações críticas e notificar a equipe responsável sobre eventos inoportunos que exigem atenção imediata.

Como é visto na Figura 6, as triggers são representadas por cores distintas, cada uma correspondendo a um grau específico de severidade. A tonalidade azul claro apenas informativa, a amarela indica um estado de atenção, enquanto a laranja denota problemas de média gravidade. Já o vermelho sinaliza ocorrências importantes, e o vermelho escuro é reservado para situações de desastre, envolvendo perdas financeiras significativas ou perda total de capacidade, entre outros desdobramentos críticos.

	Atenção	OK	ICMP Ping: ICMP: High ICMP ping response time **Depende de:** DNS Primario: ICMP: High ICMP ping loss DNS Primario: ICMP: Unavailable by ICMP ping	Value: {ITEM.LASTVALUE1}	**avg**(/DNS Primario/icmppingsec,5m)>{$ICMP_RESPONSE_TIME_WARN}	Ativo
	Alta	OK	ICMP Ping: ICMP: Unavailable by ICMP ping		**max**(/DNS Primario/icmpping,#3)=0	Ativo
	Informação	OK	Network interface discovery: Interface ens192: Ethernet has changed to lower speed than it was before **Depende de:** DNS Primario: Interface ens192: Link down	Current reported speed: {ITEM.LASTVALUE1}	Incidente: **change**(/DNS Primario/vfs.file.contents["/sys/class/net/ens192/speed"])<0 and **last**(/DNS Primario/vfs.file.contents["/sys/class/net/ens192/speed"])>0 and (**last**(/DNS Primario/vfs.file.contents["/sys/class/net/ens192/type"])=6 or **last**(/DNS Primario/vfs.file.contents["/sys/class/net/ens192/type"])=1) and (**last**(/DNS Primario/vfs.file.contents["/sys/class/net/ens192/operstate"])<>2) Recuperação: (**change**(/DNS Primario/vfs.file.contents["/sys/class/net/ens192/speed"])>0 and **last**(/DNS Primario/vfs.file.contents["/sys/class/net/ens192/speed"],#2)>0) or (**last**(/DNS Primario/vfs.file.contents["/sys/class/net/ens192/operstate"])=2)	Ativo

Figura 6. Triggers
Autoria própria

O Zabbix tem uma funcionalidade para o administrador adicionar tipos de mídias, o e-mail foi escolhido como um canal de entrega de mensagens, por ser uma

plataforma mais segura e profissional. Funciona da seguinte forma, quando uma *triggers* é acionada, uma mensagem de alerta está sendo enviada para os e-mails da equipe de Tecnologia da Informação (TI), informando aos responsáveis sobre o problema em questão. Ademais, na figura 7 mostra um exemplo da *dashboard* do Grafana que também integrou-se para receber os dados coletados e exibir gráficos detalhados sobre o desempenho e a disponibilidade dos recursos, do que o widget de gráfico do próprio Zabbix [Lambert 2019].

Figura 7. Exemplo de dashboard no Grafana
Autoria própria

4. Resultados

Os resultados alcançados incluem o desenvolvimento do sistemas de monitoramento de redes utilizando o Zabbix, implementados nos campus da UESPI em Teresina - PI (Campus Poeta Torquato Neto) e em Piripiri-PI (Campus Prof. Antônio Giovani Alves de Sousa). Esse sistema representam uma ferramenta essencial para a identificação problemas na infraestrutura de rede da instituição, proporcionando uma resposta ágil para sua resolução ou até mesmo prevenindo sua ocorrência.

Esta solução tem se mostrado eficaz para os administradores de rede, permitindo aprimorar a infraestrutura da universidade. Por meio de alertas e notificações enviadas por e-mail, os responsáveis são informados em tempo real sobre eventos críticos que afetam o desempenho da rede, possibilitando a adoção de medidas corretivas.

Conforme ilustrado na figura 8, observa-se um problema ocorrido no Campus Poeta Torquato Neto às 10:17:21 do dia 17/05/2024 na interface PALACIO_PIRAJA_ETH02, onde o link foi desativado no dispositivo MikroTik01, com gravidade classificada como média. Já na figura 9, é apresentado o processo de

resolução do problema, que foi concluído às 10:24:22 do mesmo dia, totalizando uma duração de 7 minutos e 1 segundo.

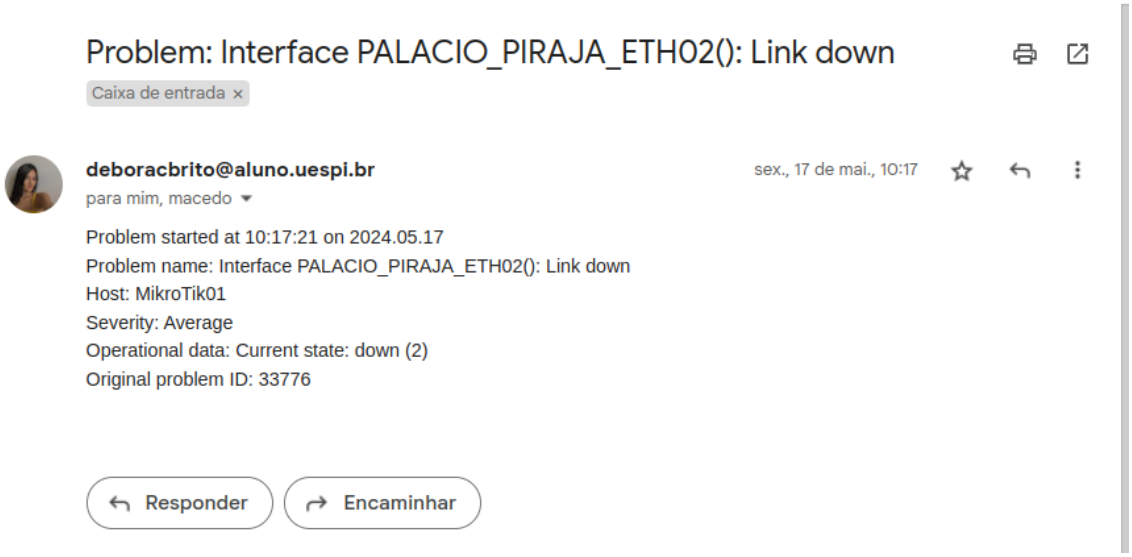

Figura 8. Notificação de problema em Teresina
Autoria própria

Figura 9. Notificação de resolução de problema em Teresina
Autoria própria

Em um ambiente acadêmico a conexão é fundamental, para a administração e estudantes. Uma queda de internet às 10h17 afeta as aulas e o funcionamento do campus. Nesse contexto, a resolução em apenas 7 minutos demonstra a importância do monitoramento e da atuação da equipe técnica, minimizando os prejuízos causados pela indisponibilidade da rede.

Na Figura 10, é notificado um problema ocorrido às 20:29:50 do dia 22/10/2024 no Campus Prof. Antônio Giovani Alves de Sousa. O servidor BancoDeDados

apresentou uma carga de CPU elevada, com uma média de uso acima do limite recomendado para um sistema com apenas uma CPU, o que pode comprometer o desempenho das operações. Porém na Figura 11, é mostrado que o problema com gravidade classificada como média foi resolvido às 20:41:50, após uma duração de 12 minutos.

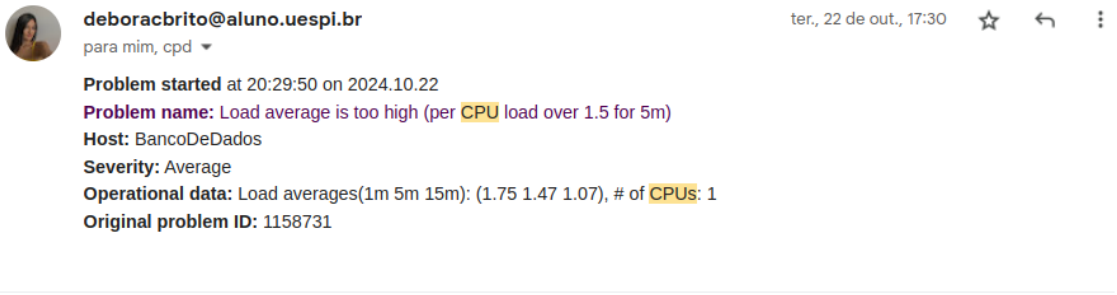

Figura 10. Notificação de problema em Piripiri
Autoria própria

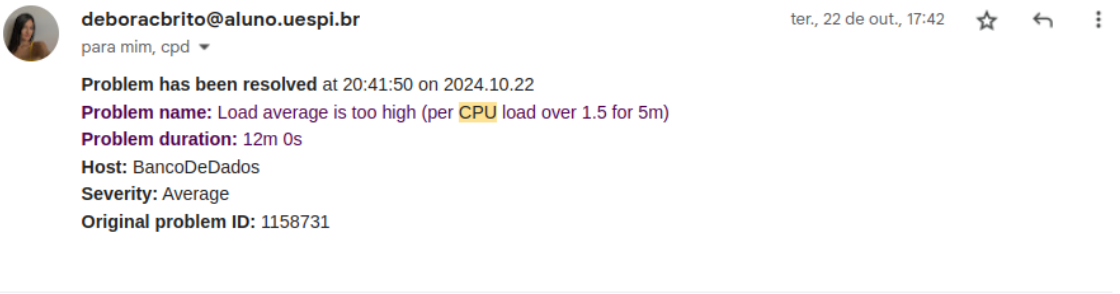

Figura 11. Notificação de resolução de problema em Piripiri
Autoria própria

Além disso, a utilização do Grafana possibilitou uma visualização mais aprofundada dos dados, proporcionando uma compreensão mais completa do estado da rede. Observou-se que essa solução tenha um impacto significativo na infraestrutura da Universidade Estadual do Piauí e que facilmente seja mantida e utilizada independentemente de quem for o administrador de rede.

A Figura 12 apresenta a *dashboard* do MikroTik, Mikrotik afirma que é um sistema operacional baseado em Linux que transforma uma plataforma x86 em um roteador, onde todo o tráfego de internet é gerenciado. Através do monitoramento, é possível escolher a data e hora que deseja visualizar as informações importantes, como o uso de processamento, espaço disponível em disco, memória, entre outros parâmetros essenciais.

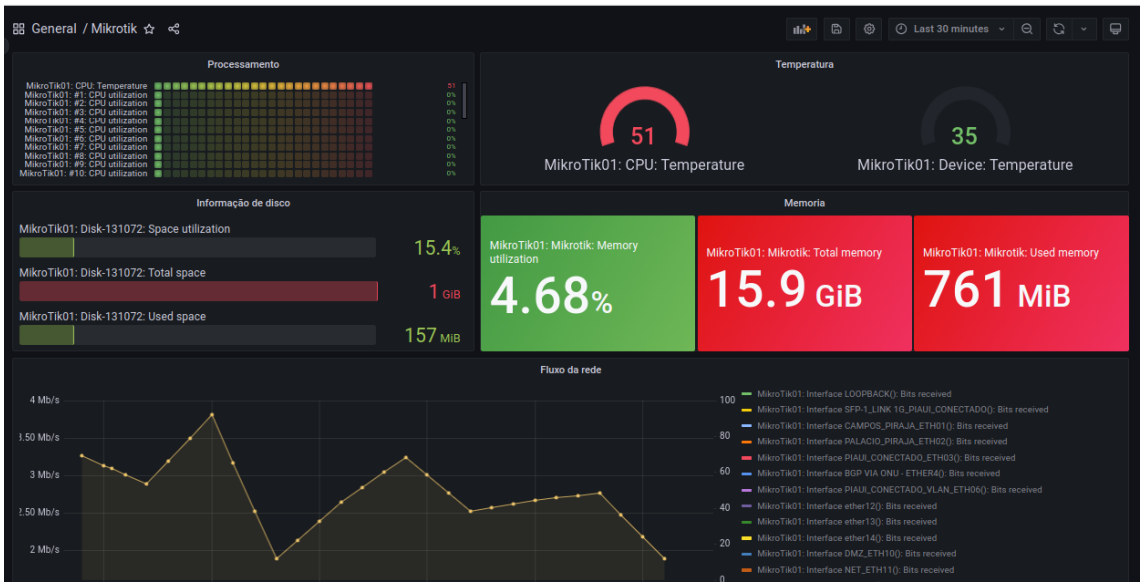

Figura 12. Dashboard da Mikrotik
Autoria própria

A dashboard exibida na Figura 13 mostra o funcionamento do DNS Primário da UESPI, é o servidor principal encarregado de gerenciar as informações para a resolução de nomes de domínio. Apartir dele que é possível o acesso a sites e serviços na web por meio de nomes, ao invés de números IP. A dashboard facilita a visualização do status, desempenho e quaisquer falhas que possam impactar o funcionamento do servidor.

Figura 13. Dashboard do DNS1
Autoria própria

Ademais, as figuras 14 e 15 são apresentadas as dashboards do Proxy Reversos 1 e Proxy Reversos 2, componentes fundamentais na infraestrutura que desempenham

funções essenciais, como a distribuição de tráfego, o gerenciamento de conexões e a proteção dos servidores contra acessos diretos. Eles garantem uma maior eficiência e segurança na comunicação entre os usuários e os serviços.

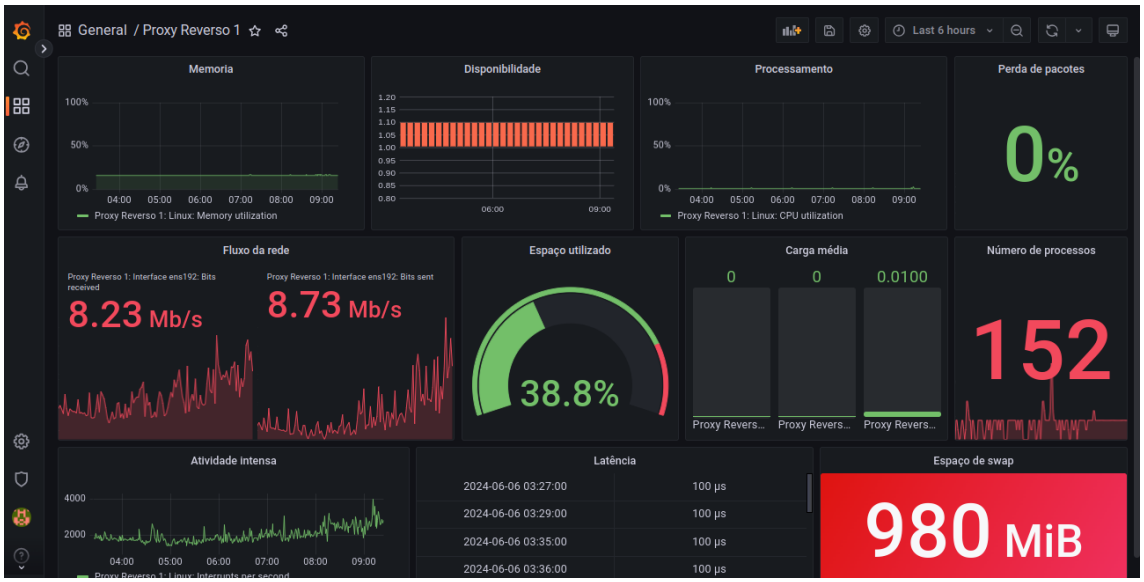

Figura 14. Dashboard do Proxy Reverso1
Autoria própria

Figura 15. Dashboard do Proxy Reverso2
Autoria própria

O monitoramento do próprio Zabbix também é crucial, para que tudo funcione em perfeito estado. A Figura 16 destaca os principais itens relacionados ao servidor da UESPI em Piripiri, enquanto a Figura 17 ilustra os itens do servidor da UESPI em Teresina. Através desses gráficos é possível identificar o fluxo de rede, processamento, espaço utilizado e memória.

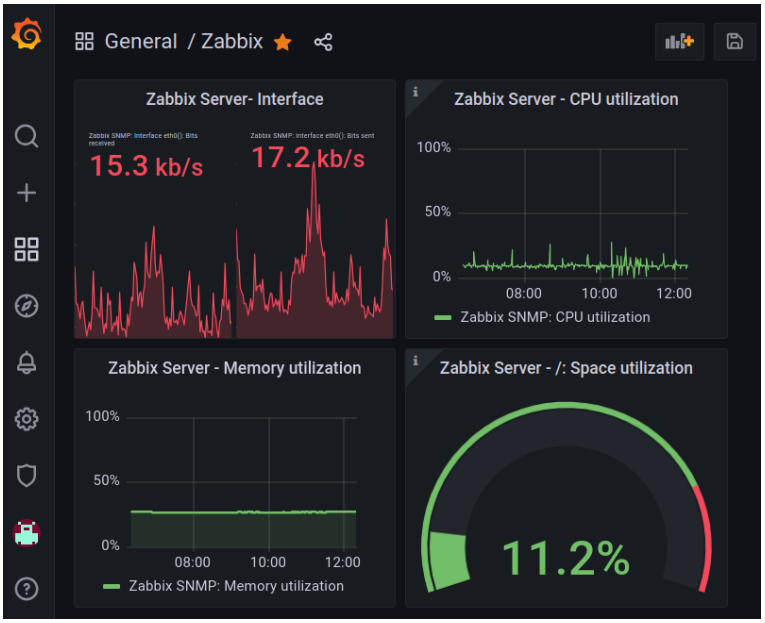

Figura 16. Dashboard do Zabbix de Piripiri
Autoria própria

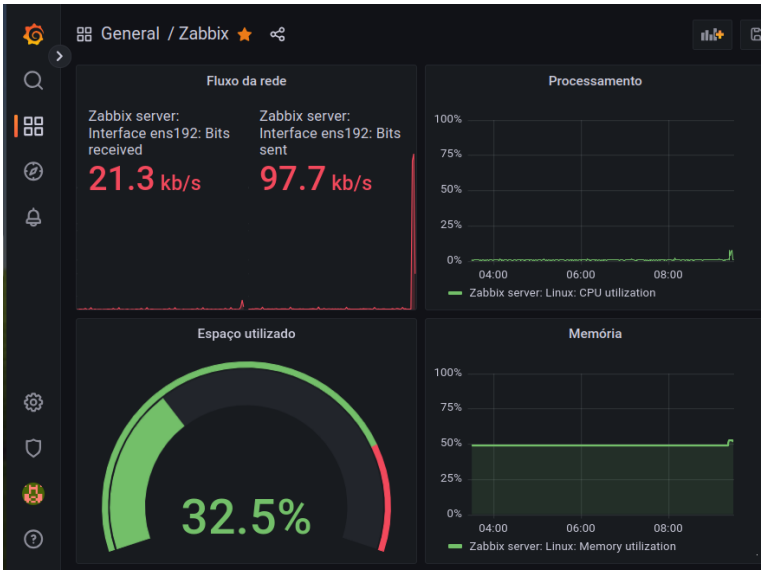

Figura 17. Dashboard do Zabbix de Teresina
Autoria própria

5. Conclusão

Considerando a ampla quantidade de tecnologias presentes no cenário atual da universidade, era evidente a necessidade de um monitoramento eficiente. A implementação do sistema de monitoramento de redes trouxe melhorias significativas para o ambiente acadêmico foi possível estabelecer uma rede mais segura e confiável. Houve feedbacks positivos da equipe de rede, que destacou o valor das notificações

geradas pelo sistema, as quais têm sido essenciais para a identificação e resolução de problemas no ambiente acadêmico.

Além disso, este trabalho também é de grande utilidade para estudantes e entusiastas da área, pois oferece informações detalhadas para o estudo e a replicação do monitoramento em diversos cenários, contribuindo para o desenvolvimento de conhecimentos técnicos e para a aplicação em situações reais.

Quanto aos trabalhos futuros, uma ideia é expandir o monitoramento para incluir ativos que não foram abordados neste projeto, garantindo uma cobertura ainda mais completa da infraestrutura de rede. Ademais, desenvolver e implementar um projeto que disponibilize uma televisão, permitindo que os administradores de rede acompanhem os gráficos em tempo real de forma contínua e centralizar os dados de todos os campus na UESPI que está localizada no Campus Poeta Torquato Neto.

Referências

Bauermann, D. (2010). Monitoramento da rede de a a zabbix. Disponível em: https://pt.slideshare.net/slideshow/monitoramento-rede/4496892#17 Acesso em: 05 de janeiro 2024.

Bueno, L. E. N. (2022). Monitoramento de dispositivos em rede utilizando zabbix e grafana. Technical report, Instituto Federal de Educação, Ciência e Tecnologia Farroupilha.

Comer, D. E. (2007). *Redes de Computadores e Internet*. Bookman, 4ª edition.

dos Santos, J. B. M., dos Santos, J. G., and de Oliveira Pereira, R. B. (2020). Monitoramento proativo e gerenciamento de rede da ufmt, usando a ferramenta zabbix. *Brazilian Journal of Development*, 6(6):38139–38146.

Fotios, R. (2021). Vazamentos de dados aumentaram 493% no brasil, mostra pesquisa do mit. Disponível em: https://cultura.uol.com.br/noticias/colunas/ricardofotios/35_vazamentos-de-dados-aumentaram-493-no-brasil-mostra-pesquisa-do-mit.html. Acesso em: 26 de julho 2023.

Lambert, D. (4 de novembro de 2019). Configurando o grafana com o zabbix. Disponível em: https://blog.zabbix.com/configuring-grafana-with-zabbix/8007/. Acesso em: 04 de janeiro 2024.

Mohr, R. F. (2012). Análise de ferramentas de monitoração de código aberto. Technical report, Universidade Federal do Rio Grande Do Sul.

Paula, J. V. G. d. et al. (2016). Implantação do zabbix no if goiano campus morrinhos. Technical report, Instituto Federal Goiano.

Shandwick, W. (2022). Estudo ibm: consumidores pagam o preço por violações de dados. Disponível em: https://www.ibm.com/blogs/ibm-comunica/estudo-ibm/#:~:text=Brasil\%2C22deagostode,relatÃČÅ§rioparaasorganizaÃČÄ§ÃČÂμespesquisadas. Acesso em: 26 de julho 2023.

SIA, Z. (2001-2024a). 2 requisitos. Disponível em: https://www.zabbix.com/documentation/5.0/en/manual/installation/requirements Acesso em: 05 de janeiro 2024.

SIA, Z. (2001-2024b). 2 requisitos. Disponível em: https://www.zabbix.com/documentation/6.0/en/manual/installation/requirements Acesso em: 05 de janeiro 2024.

SIA, Z. (2001-2024c). 3 triggers. Disponível em: https://www.zabbix.com/documentation/3.0/pt/manual/config/triggers#:~:text=As%20triggers%20s%C3%A3o%20express%C3%B5es%20l%C3%B3gicas,sistema%20em%20rela%C3%A7%C3%A3o%20aos%20mesmos. Acesso em: 04 de janeiro 2024.

SILVA, W. M. C. (2015). nálise e gerenciamento de redes usando metodologia proativa com zabbix. Technical report, HOLOS.