



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO PIAUÍ
CAMPUS PEDRO II
TECNOLOGIA EM ANÁLISE E DESENVOLVIMENTO DE SISTEMAS

ISAQUE PEREIRA FERREIRA

MONITORAMENTO PROATIVO DE REDES COM ZABBIX: estudo de caso no
IFPI – campus Pedro II

PEDRO II
2026

ISAQUE PEREIRA FERREIRA

MONITORAMENTO PROATIVO DE REDES COM ZABBIX: estudo de caso no IFPI –
campus Pedro II

Trabalho de Conclusão de Curso (artigo científico) apresentado como exigência parcial para obtenção do diploma do Curso de Análise e Desenvolvimento de Sistemas do Instituto Federal de Educação, Ciência e Tecnologia do Piauí, Campus Pedro II.

Orientador: Prof. Me. Paulo de Oliveira
Gomes Filho.

PEDRO II
2026

MONITORAMENTO PROATIVO DE REDES COM ZABBIX: estudo de caso no IFPI – campus Pedro II

Isaque Pereira Ferreira¹

Paulo de Oliveira Gomes Filho²

RESUMO

As instituições públicas e privadas são dependentes de conectividade para o desempenho de suas funções, o que torna o monitoramento de rede necessário para assegurar a qualidade dos serviços. Nesse contexto, surgem modelos de monitoramento e ferramentas que realizam essa tarefa de modo automático. O Zabbix é uma dessas ferramentas, de código aberto e amplamente utilizada em diferentes cenários. Diante disso, este trabalho teve como objetivo avaliar como a ferramenta de monitoramento Zabbix pode auxiliar no diagnóstico de problemas de conectividade no Instituto Federal do Piauí - Campus Pedro II. A pesquisa caracterizou-se como estudo de caso, no qual foi realizada a implantação do sistema, contemplando o cadastro de *hosts*, elaboração de mapa de monitoramento, desenvolvimento de *dashboards* para a visualização dos dados e a configuração de alertas por e-mail. A solução permitiu o monitoramento contínuo dos principais ativos de rede do *campus*, coleta de métricas de desempenho e disponibilidade e centralizou a visualização dessas informações. A ferramenta contribuiu para uma abordagem proativa em lidar com os problemas de infraestrutura. Dessa forma ela demonstrou-se aplicável ao contexto da instituição estudada. **Palavras-chave:** monitoramento de redes; Zabbix; SNMP; gerenciamento de redes; infraestrutura de redes.

ABSTRACT

Public and private institutions rely on connectivity to perform their functions, which makes network monitoring essential to ensuring service quality. In this context, monitoring models and tools have emerged that perform this task automatically. Zabbix is one such tool—open-source and widely used in various scenarios. Given this, the objective of this study was to evaluate how the Zabbix monitoring tool can assist in diagnosing connectivity issues at the Federal Institute of Piauí—Pedro II Campus. The research was conducted as a case study, in which the system was implemented, including the registration of *hosts*, the creation of a monitoring map, the development of *dashboards* for data visualization, and the configuration of email alerts. The solution enabled continuous monitoring of the campus's key network assets, the collection of performance and availability metrics, and centralized visualization of this information. The tool contributed to a proactive approach to addressing infrastructure issues. Thus, it proved to be applicable to the context of the institution under study. **Keywords:** network monitoring; Zabbix; SNMP; network management; network infrastructure.

Data de aprovação: 20/07/2026 (data de apresentação do TCC).

¹ Graduando em Análise e Desenvolvimento de Sistemas. Instituto Federal do Piauí – Campus Pedro II.
E-mail: pferreiraisaque@gmail.com

² Professor Mestre. Instituto Federal do Piauí – Campus Pedro II. E-mail: paulo.filho@ifpi.edu.br.

1 INTRODUÇÃO

As instituições públicas e privadas são dependentes de conectividade para o desempenho de suas atividades (Dias; Dian, 2024). Diante disso, a preocupação com o desempenho e a disponibilidade das redes, torna necessário o monitoramento de redes para diagnosticar problemas na infraestrutura, utilizando de modelos como o de gerenciamento de Falhas, Configuração, Contabilidade, Performance e Segurança (*Fault, Configuration, Accounting, Performance, Security – FCAPS*) (Boutaba; Polyrakis, 2001) e ferramentas de monitoramento automático (Ferreira *et al.*, 2025).

O Instituto Federal de Educação, Ciência e Tecnologia do Piauí (IFPI) - Campus Pedro II, onde este estudo foi realizado, oferece cursos técnicos e superiores e possui infraestrutura de rede responsável por atender os setores administrativos, laboratórios e salas de aula (CONSELHO NACIONAL DAS INSTITUIÇÕES DA REDE FEDERAL DE EDUCAÇÃO PROFISSIONAL, CIENTÍFICA E TECNOLÓGICA, 2026). Havia relatos de reclamações da comunidade acadêmica quanto à qualidade da conexão no *campus*. Com isso, surge a demanda do monitoramento contínuo dos ativos de rede do *campus* para identificação de falhas e degradação do desempenho (Dias; Dian, 2024).

Dentre as ferramentas utilizadas para esse propósito, destaca-se o Zabbix, uma solução de código aberto amplamente empregada em ambientes corporativos e acadêmicos, que oferece suporte ao monitoramento de diferentes tipos de dispositivos de rede, justificando sua adoção neste trabalho (Calú *et al.*, 2020; Dias; Dian, 2024).

Nesse contexto, este trabalho busca avaliar como o Zabbix pode auxiliar no monitoramento para diagnóstico de problemas de conectividade no IFPI - Campus Pedro II. Para alcançar este objetivo, definiram-se os seguintes objetivos específicos:

- realizar o cadastro dos *hosts*;
- elaborar o mapa lógico de monitoramento;
- desenvolver *dashboards* para monitoramento;
- configurar alertas por e-mail;
- analisar as métricas coletadas.

A relevância desta pesquisa reside na adoção do monitoramento proativo da infraestrutura de rede, permitindo a identificação antecipada de falhas e a coleta contínua de métricas de disponibilidade, latência, perda de pacotes e utilização dos enlaces. Em contraste com a abordagem reativa, essa estratégia fornece subsídios para diagnósticos mais precisos e para a tomada de decisões fundamentadas na administração da rede (Dias; Dian, 2024).

A contribuição deste trabalho não está na originalidade do uso da ferramenta Zabbix, já consolidada em outros contextos, conforme discutido na seção de trabalhos relacionados, mas sim na aplicação específica ao ambiente do IFPI – Campus Pedro II. A pesquisa centralizou os principais ativos de rede do *campus*, mapeou os eventos de falhas e estabeleceu uma base para o monitoramento proativo da infraestrutura institucional.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 GERENCIAMENTO DE REDES

Segundo Boutaba e Polyrakis (2001), o gerenciamento de redes compreende as atividades de monitoramento e controle da infraestrutura, com o objetivo de assegurar seu funcionamento adequado. Dentre as atividades de gerenciamento de redes, destaca-se o monitoramento dos ativos da infraestrutura, o qual pode ser organizado segundo áreas funcionais definidas pelo modelo FCAPS proposto pela Organização Internacional de Padronização (*ISO - International Organization for Standardization*), cujas áreas são:

- Gerenciamento de Falhas (*Fault Management*): compreende a detecção, isolamento, correção e registro de erros que ocorrem dentro da rede;
- Gerenciamento de Configuração (*Configuration Management*): compreende a manutenção de informações precisas sobre a configuração da rede e o controle de parâmetros relacionados à sua operação normal;
- Gerenciamento de Contabilidade/Tarifação (*Accounting Management*): compreende a gestão dos usuários, bem como a contabilização e o controle do uso dos recursos e serviços;
- Gerenciamento de Desempenho (*Performance Management*): compreende a maximização do desempenho da rede. Está relacionado ao fornecimento de Qualidade de Serviço (*Quality of Service - QoS*) e a parâmetros como utilização de recursos, atraso (*delay*), variação do atraso (*jitter*) e perda de pacotes;
- Gerenciamento de Segurança (*Security Management*): compreende a garantia da segurança da rede.

Segundo Ferreira *et al.* (2025), as ferramentas de monitoramento gerenciam ativos de rede que trazem ou geram valor para uma organização, contemplando uma área funcional específica conforme classificação proposta pelo modelo FCAPS.

2.2 PROTOCOLO SNMP

O Protocolo Simples de Gerenciamento de Rede (Simple Network Management Protocol - SNMP) constitui um dos principais padrões utilizados para o monitoramento de

dispositivos que não possuem um agente nativo de monitoramento (Calú *et al.*, 2020).

Por ser um protocolo aberto, sua adoção pelos fabricantes foi facilitada. O SNMP possui uma arquitetura cliente/servidor composta por três componentes principais (Boyko; Varkentin; Polyakova, 2019):

- Estação de Gerenciamento de Redes (*NMS - Network Management Station*): sistema central que consulta os agentes e recebe alertas;
- Agentes: *softwares* instalados nos dispositivos gerenciados (como roteadores e *switches*) responsáveis por coletar informações e responder às consultas;
- Base de Informações de Gerenciamento (*Management Information Base - MIB*): uma base de dados hierárquica que define as informações disponíveis para consulta em cada dispositivo, organizadas por Identificadores de Objetos (*Object Identifier - OID*).

O SNMP possui três versões, cada uma aumentando o nível de segurança, mas com custo maior de processamento por conta da criptografia (Boyko; Varkentin; Polyakova, 2019).

2.3 ZABBIX

Para realizar esse monitoramento, ferramentas implementam os conceitos anteriormente apresentados, uma dessas é o Zabbix, sendo de código aberto, desenvolvida e mantida atualmente pela Zabbix SIA (Silva, 2021; ZABBIX SIA, 2026a). Entre suas principais características destacam-se sua flexibilidade de se adequar às necessidades específicas de cada cenário, bom desempenho, suporte a diferentes tipos de dispositivos e boa integração com serviços de terceiros, além de uma interface amigável para operar os dispositivos monitorados (Silva, 2021; Brito; Sousa, 2025).

A sua arquitetura, como aponta Ferreira *et al.* (2025), se divide em quatro componentes principais: servidor, banco de dados, interface web e agente. O servidor é a parte central que recebe e processa os dados enviados pelos agentes. O banco de dados armazena as configurações e coleções de dados. A interface web permite realizar configurações e monitorar a infraestrutura. O agente que é instalado no dispositivo e monitora os recursos a serem enviados para o servidor. O Zabbix disponibiliza um programa *Zabbix Agent* que pode ser instalado em múltiplos sistemas operacionais (ZABBIX SIA, 2026b). Quando a instalação do agente não é possível, o sistema ainda oferece suporte ao SNMP, IPMI (*Intelligent Platform Management Interface*), JMX (*Java Management Extensions*), monitoramento VMware, ICMP (*Internet Control Message Protocol*) Ping e SSH (*Secure Shell*) (Calú *et al.*,

2020).

2.4 TRABALHOS RELACIONADOS

Durante a revisão bibliográfica foram identificados trabalhos relacionados, entre eles o de Calú *et al.* (2020), que apresenta um estudo de caso de implantação do Zabbix na Universidade Federal de Alagoas (UFAL) – Campus Arapiraca, destacando-se pelo nível de detalhamento técnico e customização de OIDs proprietários. O Zabbix auxiliou no diagnóstico de problemas de infraestrutura por meio de *dashboards* e a criação de um mapa de monitoramento, no entanto não é citado o uso de alertas via e-mail ou outro tipo de mídia.

Silva e Silva (2024) enfatizam a implementação do Zabbix com segurança, devido à estrutura complexa que comportava dados sensíveis dos clientes de uma empresa de Tecnologia da Informação (TI) de soluções de gestão comercial, que atuava em diferentes municípios da região metropolitana de Campina, havendo a necessidade do uso de um sistema de Rede Privada Virtual (*Virtual Private Network - VPN*).

Brito e Sousa (2025) relatam outro estudo de caso onde o Zabbix foi usado para monitorar a infraestrutura de rede da Universidade Estadual do Piauí (UESPI) – Campus Poeta Torquato Neto (Teresina – PI) e Campus Prof. Antônio Giovani Alves de Sousa (Piripiri – PI), trouxeram a configuração de alertas via e-mail e integração com o Grafana, demonstrando como o sistema auxiliou no rápido diagnóstico de problemas da instituição. Em trabalhos futuros espera-se ampliar o número de *hosts* monitorados e a utilização de um aparelho televisor para visualização dos *dashboards* pela equipe de Tecnologia da Informação.

Semelhantemente, Silva (2021) propõe uma integração Zabbix e Grafana, com a diferença do uso de canais de mensageria instantânea (Telegram) também suportado pelo Zabbix, garantindo que o administrador receba alertas rapidamente. Além disso, o autor interliga o Grafana via conexão direta ao banco de dados (*Direct DB*), diminuindo a latência de requisições para gerar os gráficos para visualização.

Já Ferreira *et al.* (2025) propõem uma implementação robusta de Zabbix, Grafana e ZeroTier dentro de um ambiente virtualizado com contêineres LXC (*Linux containers*) no *Proxmox VE*, aplicado no Laboratório de Redes de Computadores (CNL) da Universidade Estadual do Mato Grosso (UNEMAT). O ZeroTier permite o gerenciamento remoto seguro sendo mais simples que VPNs tradicionais, aliado à correção de métricas de hardware dentro do ambiente containerizado. Ademais, os autores validaram a responsividade e a acurácia dos *dashboards* gerados por meio de testes de injeção de tráfego com a ferramenta *Iperf3*,

demonstrando que a arquitetura é viável, precisa e aplicável tanto para fins corporativos quanto acadêmicos.

Dias e Dian (2024) complementam com outros estudos de caso, incluindo de corporações e órgãos públicos espalhados ao redor do mundo, além de história e evolução da ferramenta, como também os seus diferenciais competitivos em relação aos concorrentes.

Em conjunto, esses estudos demonstram a viabilidade da utilização do Zabbix em diferentes contextos, fornecendo embasamento para sua adoção no Instituto Federal do Piauí – Campus Pedro II. O Quadro 1 sintetiza os principais aspectos dos trabalhos relacionados, destacando as diferenças em relação à proposta desenvolvida neste estudo.

Quadro 1 — Comparação dos trabalhos relacionados.

Trabalho	Ambiente	Recursos utilizados	Forma de avaliação	Principais resultados	Diferença em relação a este trabalho
Calú <i>et al.</i> (2020)	UFAL – Campus Arapiraca	Zabbix, customização de OIDs proprietários	Estudo de caso técnico	Diagnóstico via <i>dashboards</i> e mapa de monitoramento	Não relata uso de alertas por e-mail; o presente trabalho incorpora esse mecanismo
Silva e Silva (2024)	Empresa de TI de gestão comercial (região metropolitana de Campina)	Zabbix integrado a VPN	Estudo de caso voltado à segurança	Proteção de dados sensíveis de clientes em ambiente corporativo	Ambiente corporativo com foco em segurança de dados; o presente trabalho é institucional/educacional e não utiliza VPN
(Brito; Sousa, 2025)	UESPI – Campus Poeta	Zabbix, alertas por e-mail,	Estudo de caso institucional	Diagnóstico ágil de	Ambiente mais próximo ao

	Torquato Neto e Campus Prof. Antônio Giovani	integração com Grafana		problemas; trabalhos futuros incluem mais <i>hosts</i> e TV para <i>dashboards</i>	deste estudo; a integração com Grafana ainda não foi implementada aqui, ficando como trabalho futuro
Silva (2021)	Não especificado (proposta técnica)	Zabbix, Grafana, Telegram, conexão <i>Direct DB</i>	Proposta de arquitetura	Redução da latência de requisições para geração de gráficos	Utiliza Telegram como canal de alerta em vez de e-mail; não há uso de conexão direta ao banco de dados no presente trabalho
Ferreira <i>et al.</i> (2025)	UNEMAT – Laboratório CNL, ambiente virtualizado em Proxmox VE (LXC)	Zabbix, Grafana, ZeroTier, testes com Iperf3	Testes de injeção de tráfego e validação de acurácia dos <i>dashboards</i>	Arquitetura validada como viável, precisa e aplicável	Compartilha o uso do Proxmox VE como base de virtualização, mas não realizou testes de tráfego com Iperf3, ficando como trabalho futuro
Dias e Dian (2024)	Revisão de casos internacionais	Não aplicável (revisão bibliográfica)	Revisão da literatura	Panorama histórico e evolutivo da	Não é um estudo de implantação

	(corporações e órgãos públicos)			ferramenta	prática como o presente trabalho, mas fundamenta teoricamente a relevância do Zabbix
--	---------------------------------	--	--	------------	--

Fonte: Do autor (2026).

3 METODOLOGIA

Esta pesquisa caracteriza-se como aplicada, pois busca solucionar um problema prático relacionado ao monitoramento da infraestrutura de rede do IFPI – Campus Pedro II. Quanto à abordagem, possui caráter predominantemente quantitativo e descritivo, uma vez que se fundamenta na coleta e análise de métricas objetivas — como disponibilidade, latência, perda de pacotes e volume de eventos — obtidas por meio da ferramenta de monitoramento. Em relação aos procedimentos técnicos, trata-se de um estudo de caso, desenvolvido em ambiente real, conforme a definição de Yin (2015), permitindo investigar a aplicação do Zabbix no contexto específico da instituição.

O estudo foi desenvolvido no Instituto Federal de Educação, Ciência e Tecnologia do Piauí (IFPI) – Campus Pedro II, unidade pertencente à Rede Federal de Educação Profissional, Científica e Tecnológica, cuja infraestrutura de rede atende às atividades administrativas e acadêmicas da instituição (CONSELHO NACIONAL DAS INSTITUIÇÕES DA REDE FEDERAL DE EDUCAÇÃO PROFISSIONAL, CIENTÍFICA E TECNOLÓGICA, 2026). O ambiente é composto principalmente pelos seguintes equipamentos: *firewall pfSense* (NETGATE, 2026), *switches HP* e *TP-Link*, *access points Cisco*, servidores Linux e impressoras, que sustentam os serviços de conectividade utilizados pela comunidade acadêmica.

A escolha do IFPI – Campus Pedro II como ambiente de estudo deve-se à disponibilidade da infraestrutura necessária para implantação da solução e à necessidade de avaliar a aplicação do Zabbix em um ambiente institucional real. Havia relatos de reclamações da comunidade acadêmica quanto à qualidade da conexão no campus, confirmados durante o desenvolvimento do projeto por meio do acompanhamento da rotina do Centro de Tecnologia da Informação (CTI) do *campus*, permitindo verificar sua utilização no monitoramento dos ativos de rede do *campus*. Antes do início da implementação, o

ambiente de monitoramento havia sido instalado, com os componentes principais do Zabbix configurados em uma máquina virtual executando no *Proxmox VE* (PROXMOX SERVER SOLUTIONS GMBH, 2026). Foram alocados ao servidor Zabbix 2 núcleos de processamento, 4 GB de memória RAM e 60 GB de armazenamento. O Quadro 2 sintetiza os principais aspectos metodológicos do monitoramento realizado.

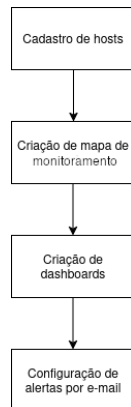
Quadro 2 – Aspectos metodológicos do monitoramento

Elemento	Informação
Período de monitoramento	Aproximadamente duas semanas, contabilizado a partir da consolidação de todos os <i>hosts</i> no ambiente, incluindo o enlace de internet do <i>campus</i> , cadastrado em etapa posterior aos demais equipamentos
Versão do Zabbix	7 LTS
Requisitos de sistema do servidor	CPU: 2; memória RAM: 4GB; armazenamento: 60 GB.
Quantidade de <i>hosts</i>	38
Protocolos utilizados	SNMP e agente Zabbix (<i>passive</i>)
Intervalo de coleta	Padrão dos <i>templates</i> nativos do Zabbix, conforme o tipo de item monitorado (agente ou ICMP <i>ping</i>), sem customização adicional
Critérios de indisponibilidade	Definidos pelos <i>triggers</i> padrão dos <i>templates</i> nativos aplicados a cada <i>host</i> , sem customização adicional
Forma de análise	Estatística descritiva e análise dos eventos registrados no sistema

Fonte: Do autor (2026).

Dessa forma, este trabalho concentrou-se nas seguintes etapas: cadastro dos *hosts*, elaboração do mapa lógico de monitoramento, desenvolvimento dos *dashboards* de monitoramento e configuração dos alertas por e-mail. A Figura 1 apresenta as etapas adotadas durante a implementação.

Figura 1 – Abordagem de implementação.



Fonte: Do autor (2026).

No cadastro dos *hosts* foi atribuído um nome único, um grupo e um *template* compatível para cada equipamento. Também foram configurados o endereço IP e o tipo de agente responsável pela coleta das métricas (ZABBIX SIA, 2026b), como exemplificado na Figura 2. Durante essa etapa foi identificado o bloqueio do tráfego proveniente do servidor Zabbix pelo *firewall pfSense* da instituição. Para solucionar esse problema, foi criada uma regra específica permitindo a comunicação entre os dispositivos monitorados e o servidor Zabbix.

Após o cadastramento dos dispositivos, foi elaborado o mapa lógico de monitoramento da infraestrutura de rede do *campus*. O mapa permitiu identificar visualmente falhas por meio da severidade dos eventos (Calú *et al.*, 2020), conforme apresentado na Figura 3.

Figura 2 – Cadastro de um novo *host*.

A imagem mostra a interface web do Zabbix para o cadastro de um novo host. O título da página é 'Servidor'. Abaixo dele, há uma barra de navegação com links: 'Servidor', 'IPMI', 'Etiquetas', 'Macros', 'Inventário', 'Encriptação' e 'Mapeamento de valores'. O link 'Servidor' está selecionado.

Na seção principal, há os seguintes campos e opções:

- * Nome do host:** Um campo de texto com o valor 'SWITCHPII01'.
- Nome visível:** Um campo de texto com o valor 'SWITCHPII01'.
- Templates:** Uma tabela com duas colunas: 'Nome' e 'Acção'.

Nome	Acção
HP Comware HH3C by SNMP	Desassociar Desassociar e eliminar

 Abaixo da tabela, há um campo de busca 'digite aqui para pesquisar' e um botão 'Seleccionar'.
- * Grupos de hosts:** Um campo de busca com o valor 'Switches' e um ícone de fechar. Abaixo dele, há um campo de busca 'digite aqui para pesquisar' e um botão 'Seleccionar'.
- Interfaces:** Uma tabela com as seguintes colunas: 'Tipo', 'Endereço IP', 'Nome DNS', 'Ligado a', 'Porto' e 'Por omissão'.

Tipo	Endereço IP	Nome DNS	Ligado a	Porto	Por omissão
SNMP			IP DNS	161	☒ Eliminar

 Abaixo da tabela, há um link 'Adicionar'.

Fonte: Do autor (2026).

configurar os alertas foi cadastrado um e-mail dedicado para os alertas do Zabbix, que depois foi associado ao usuário administrador e então foi criada a ação (*Action*) de envio do alerta por e-mail (Brito; Sousa, 2025).

A avaliação da solução foi realizada considerando quatro critérios: (i) capacidade de monitorar continuamente os ativos de rede; (ii) coleta de métricas de disponibilidade e desempenho; (iii) visualização das informações por meio de *dashboards*; e (iv) funcionamento do mecanismo de envio automático de alertas por e-mail. Os resultados obtidos foram analisados à luz da literatura relacionada, especialmente estudos que empregaram o Zabbix em ambientes institucionais semelhantes.

Não foram realizados testes de estresse ou geração artificial de tráfego, uma vez que o objetivo do estudo concentrou-se na avaliação da capacidade da ferramenta em monitorar continuamente a infraestrutura existente.

4 RESULTADOS

Os resultados obtidos neste trabalho concentram-se principalmente em duas das cinco áreas funcionais do modelo FCAPS apresentado na fundamentação teórica: o Gerenciamento de Falhas, evidenciado pelo registro e classificação dos eventos de indisponibilidade e pela configuração dos alertas automáticos; e o Gerenciamento de Desempenho, refletido na coleta de métricas de disponibilidade, latência, perda de pacotes e utilização de recursos computacionais (Boutaba; Polyrakis, 2001). As demais áreas do modelo — Configuração, Contabilidade e Segurança — não constituíram foco da implementação, sendo indicadas como possibilidades de expansão em trabalhos futuros.

Durante o período de monitoramento, foram cadastrados 38 *hosts*, sendo 4 monitorados via agente Zabbix (passive) e 34 via protocolo SNMP. Do total, 35 *hosts* (92,1%) permaneceram disponíveis, enquanto 3 apresentaram indisponibilidade em algum momento do período analisado, conforme detalhado na Tabela 1. Os equipamentos monitorados via SNMP apresentaram disponibilidade de 94,1%, ligeiramente superior à dos monitorados via agente (75,0%), o que pode estar relacionado à menor quantidade de *hosts* nessa categoria, tornando cada indisponibilidade proporcionalmente maior.

É importante destacar que os percentuais apresentados na Tabela 1 refletem a proporção de *hosts* que permaneceram disponíveis durante todo o período analisado, e não uma medida de disponibilidade ponderada pelo tempo efetivo de indisponibilidade de cada equipamento. Um *host* que apresentou uma breve indisponibilidade é contabilizado da mesma forma que outro com indisponibilidade prolongada, o que é indicado como ponto de melhoria

metodológica para trabalhos futuros.

Tabela 1 – Situação dos *hosts* durante o período de monitoramento.

Tipo de agente	Total	Disponíveis	Indisponíveis	Disponibilidade (%)
<i>Agent (passive)</i>	4	3	1	75,0%
SNMP	34	32	2	94,1%
Total	38	35	3	92,1%

Fonte: Do autor (2026).

Em relação aos eventos de falha, o mapa lógico de monitoramento (Figura 3) registrou um total de 142 problemas identificados nos *switches* e servidores monitorados durante o período do estudo, evidenciando a ocorrência recorrente de instabilidades em nível de interface, principalmente em equipamentos do tipo *switch*. Esse volume de eventos reforça a utilidade do monitoramento contínuo para identificação de padrões de falha que, de outra forma, dependeriam de relatos informais da comunidade acadêmica para serem percebidos.

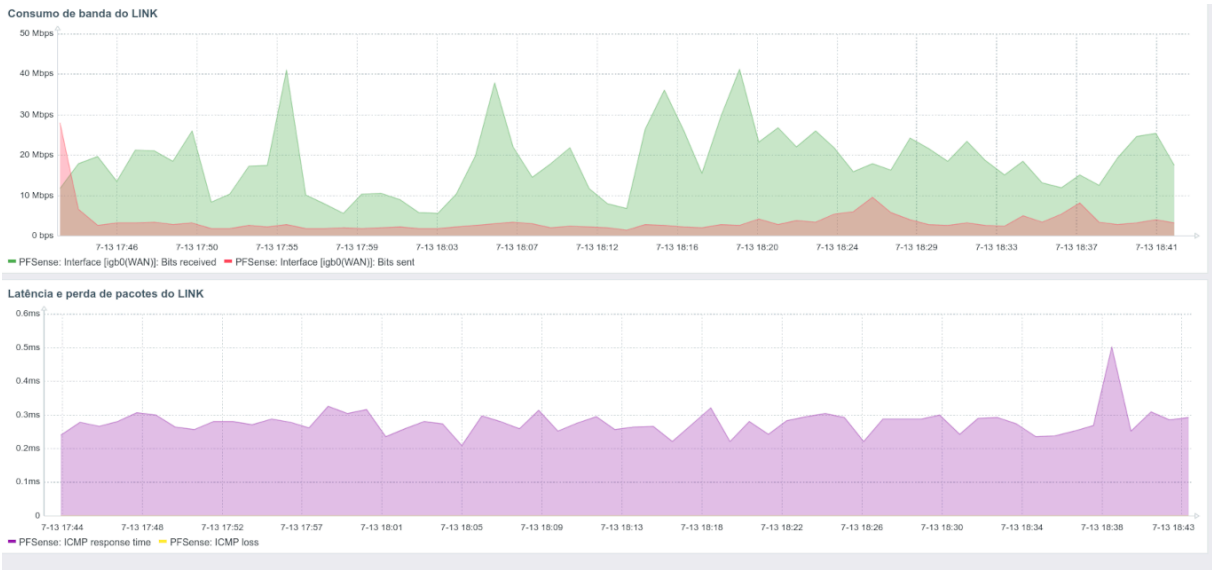
A Figura 5 apresenta as principais métricas coletadas do enlace de internet do *campus* por meio do protocolo SNMP. As informações incluem utilização da largura de banda, latência e perda de pacotes, permitindo acompanhar continuamente o comportamento do *link* principal da instituição.

Observou-se baixa utilização do enlace, latência variando entre aproximadamente 25 e 30 ms e ausência de perda significativa de pacotes. Esses resultados indicam que, no período analisado, não houve evidências de saturação da banda contratada, sugerindo que eventuais problemas de conectividade podem estar relacionados a outros componentes da infraestrutura de rede.

Resultado semelhante foi observado por Brito e Sousa (2025), que utilizaram o Zabbix para acompanhar métricas de desempenho em ambientes institucionais, demonstrando a utilidade da ferramenta na identificação de gargalos da infraestrutura.

A Figura 6 apresenta o *widget* de problemas do Zabbix, responsável por consolidar os eventos detectados nos dispositivos monitorados. Esse recurso permite identificar rapidamente equipamentos indisponíveis ou com comportamento anômalo, classificando os eventos conforme seu nível de severidade.

Figura 5 – Gráficos do link.



Fonte: Do autor (2026).

Figura 6 – Widget de Problemas.

Problemas								
Time ▼	Recovery time	Estado	Informação	Servidor	Problema • Severidade	Duração	Atualizar	Ações
18:26:17		PROBLEMA	SWITCHP11 10	HP Enterprise Switch: Interface Ethernet1/0/3(Ethernet1/0/3 Interface): Link down	12m 24s	Atualizar	1	→
18:24:50		PROBLEMA	SWITCHP11 02	HP Comware HH3C: Interface GigabitEthernet1/0/19(GigabitEthernet1/0/19 Interface): Link down	13m 51s	Atualizar	1	→
18:22:17		PROBLEMA	Zabbix server	Linux: Load average is too high (per CPU load over 1.5 for 5m)	16m 24s	Atualizar	1	→
18:13:16		PROBLEMA	SWITCHP11 09	HP Comware HH3C: Interface GigabitEthernet1/0/5(GigabitEthernet1/0/5 Interface): Link down	25m 25s	Atualizar	1	→

Fonte: Do autor (2026).

A centralização dessas informações reduz o tempo necessário para localizar a origem de falhas, permitindo que a equipe técnica priorize os incidentes mais críticos. Essa funcionalidade está alinhada ao conceito de monitoramento proativo discutido por Dias e Dian (2024).

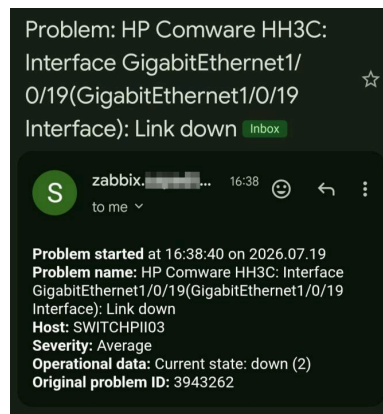
Figura 7 apresenta parte das métricas coletadas do servidor UniFi (UBIQUITI INC., 2026), como utilização de CPU, memória e carga de sistema.

O acompanhamento contínuo dessas informações permite identificar tendências de utilização dos recursos computacionais e antecipar possíveis degradações de desempenho, contribuindo para o planejamento das atividades de manutenção.

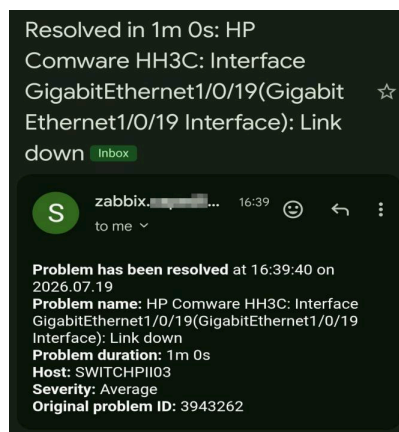
Figura 7 – Gráficos servidor UniFi.



Fonte: Do autor (2026).

Figura 8 – E-mail sobre falha em *switch*.

Fonte: Do autor (2026).

Figura 9 – E-mail sobre falha em *switch* – Resolvido.

Fonte: Do autor (2026).

Após a configuração das ações do Zabbix, os eventos classificados como problemas passaram a gerar notificações automáticas por e-mail destinadas ao administrador da rede, conforme ilustrado nas Figuras 8 e 9.

Com base nas notificações automáticas geradas pelo Zabbix, foi possível calcular o tempo de resolução de uma amostra de eventos registrados durante o período de monitoramento. O tempo médio de resolução (*Mean Time To Resolution – MTTR*) foi de aproximadamente 5,75 minutos, variando entre 1 e 17 minutos conforme a natureza do evento. Esse resultado demonstra que a maior parte das ocorrências foi de curta duração, sugerindo instabilidades pontuais nas interfaces de rede, e evidencia a contribuição do mecanismo de alertas por e-mail para a rápida identificação e resposta a esses eventos, corroborando o conceito de monitoramento proativo discutido por Dias e Dian (2024).

Esse mecanismo reduz a dependência do acompanhamento contínuo da interface web do sistema, permitindo que a equipe responsável seja informada imediatamente sobre alterações no estado dos dispositivos monitorados, sugerindo que esse mecanismo pode contribuir para a redução do tempo de resposta diante de incidentes, embora esse ganho não tenha sido mensurado diretamente em relação a um cenário anterior sem alertas automáticos (Brito; Sousa, 2025).

Durante a realização do projeto limitações apareceram, como o prazo menor que inviabilizou a coleta por um período de tempo maior, faltando dados para chegar a um diagnóstico dos problemas que a instituição enfrenta. Também na verificação do *link* seria necessário o uso de ferramentas para injeção de tráfego (Ferreira *et al.*, 2025). No entanto, isso não afeta o papel do Zabbix, que continua a fornecer informações sobre o estado da infraestrutura do *campus*.

De modo geral, os resultados demonstram que os objetivos propostos foram alcançados. A solução implementada possibilitou o monitoramento contínuo dos ativos da infraestrutura, a centralização das informações em *dashboards*, a visualização de falhas na infraestrutura de rede e o envio automático de alertas, confirmando a aplicabilidade do Zabbix como ferramenta de apoio ao diagnóstico de problemas de conectividade no IFPI – Campus Pedro II.

5 CONSIDERAÇÕES FINAIS

Este trabalho teve como objetivo avaliar a capacidade da ferramenta de monitoramento de rede Zabbix para auxiliar no diagnóstico de problemas de conexão do Instituto Federal do Piauí – Campus Pedro II.

Para atingir este objetivo, foi realizada a implantação da solução compreendendo as etapas de cadastro de *hosts*, elaboração de mapa lógico de monitoramento, construção de *dashboards* e alertas automáticos por e-mail. Os resultados obtidos demonstram que a ferramenta foi capaz de monitorar continuamente os dispositivos de rede, coletar métricas de disponibilidade e desempenho, além de notificar o administrador sobre ocorrências de eventos.

A implantação do Zabbix demonstrou que a ferramenta é tecnicamente viável para centralizar informações, detectar eventos, acompanhar métricas de desempenho e emitir alertas automáticos no contexto do IFPI – Campus Pedro II. Em razão do período limitado de coleta, os resultados obtidos não permitem ainda um diagnóstico completo dos problemas de conectividade enfrentados pela instituição, mas constituem uma base consistente para diagnósticos futuros mais aprofundados, a serem conduzidos a partir da continuidade do monitoramento.

Nesse sentido, a contribuição do trabalho está menos na novidade da ferramenta empregada e mais na sua adaptação ao contexto do *campus*, consolidando em um único ambiente a visibilidade dos ativos de rede que antes dependia de verificações pontuais e relatos informais da comunidade acadêmica.

Os resultados também colaboram com a literatura consultada, que aponta o Zabbix como uma solução amplamente utilizada no monitoramento de redes em diferentes escalas e nichos, evidenciando sua adaptabilidade (Dias; Dian, 2024).

5.1 TRABALHOS FUTUROS

Para trabalhos futuros, recomenda-se: a integração com Grafana (GRAFANA LABS, 2026) para melhor visualização das métricas; uso do *Iperf3* (ESNET, 2026) para testes de injeção de tráfego; ampliação do período de coleta, com recálculo da disponibilidade considerando o tempo efetivo de indisponibilidade por equipamento; a classificação sistemática dos eventos detectados, verificando inclusive falsos positivos; a documentação de casos de resolução concretos do *campus*; extensão para monitoramento de rede sem fio; ajustes em *triggers*; elaboração de relatórios periódicos; estabelecimento de Acordos de Nível de Serviço (Service Level Agreement – SLA); e a comparação do tempo de resposta da equipe antes e depois da ferramenta.

DECLARAÇÃO DO USO DE INTELIGÊNCIA ARTIFICIAL

Durante a preparação deste manuscrito, o autor utilizou a ferramenta de Inteligência Artificial Claude (Anthropic), em julho de 2026, para revisão ortográfica, gramatical e de

consistência textual, além de apoio na redação de ajustes solicitados pela banca avaliadora. Todo o conteúdo foi revisado criticamente pelo autor, que assume total responsabilidade pela integridade científica, originalidade e ética da publicação.

REFERÊNCIAS

- BOUTABA, R.; POLYRAKIS, A. Projecting FCAPS to active networks. *In: ENTERPRISE NETWORKING, APPLICATIONS AND SERVICES CONFERENCE* (EntNet@Supercomm), 2001, Atlanta. **Proceedings [...]**. IEEE, 2001. p. 97–104. DOI: <https://doi.org/10.1109/ENTNET.2001.981995>. Disponível em: <https://ieeexplore.ieee.org/document/981995>. Acesso em: 13 mai. 2026.
- BOYKO, A.; VARKENTIN, V.; POLYAKOVA, T. Advantages and disadvantages of the data collection's method using SNMP. *In: INTERNATIONAL MULTI-CONFERENCE ON INDUSTRIAL ENGINEERING AND MODERN TECHNOLOGIES (FarEastCon)*, 2019, Vladivostok. **Proceedings [...]**. IEEE, 2019. p. 1–5. DOI: <https://doi.org/10.1109/FarEastCon.2019.8934069>. Disponível em: <https://ieeexplore.ieee.org/document/8934069>. Acesso em: 27 abr. 2026.
- BRITO, Débora Cristina Santos de; SOUSA, José Vigno Moura. **Implementação do monitoramento de redes com Zabbix**. 2025. Trabalho de Conclusão de Curso (Bacharelado em Ciências da Computação) – Universidade Estadual do Piauí, Piripiri, 2025. Disponível em: <https://sistemas2.uespi.br/handle/tede/1741>. Acesso em: 11 jul. 2026.
- CALÚ, José Junio *et al.* Implantação do Zabbix na UFAL Campus Arapiraca. *In: ESCOLA REGIONAL DE INFORMÁTICA DE GOIÁS (ERI-GO)*, 8., 2020, Evento Online. **Anais [...]**. Porto Alegre: Sociedade Brasileira de Computação, 2020. p. 171–180. DOI: <https://doi.org/10.5753/erigo.2020.13871>. Disponível em: <https://sol.sbc.org.br/index.php/erigo/article/view/13871>. Acesso em: 18 mar. 2026.
- CONSELHO NACIONAL DAS INSTITUIÇÕES DA REDE FEDERAL DE EDUCAÇÃO PROFISSIONAL, CIENTÍFICA E TECNOLÓGICA. Instituto Federal do Piauí. **CONSELHO NACIONAL DAS INSTITUIÇÕES DA REDE FEDERAL DE EDUCAÇÃO PROFISSIONAL, CIENTÍFICA E TECNOLÓGICA**, 2026. Disponível em: <https://portal.redefederal.org.br/nordeste/pi/instituto-federal-do-piaui>. Acesso em: 16 jul. 2026.
- DIAS, Gustavo; DIAN, Mauricio de Oliveira. Importância do Zabbix como uma solução de monitoramento de rede. **Revista Interface Tecnológica**, Taquaritinga, SP, v. 21, n. 2, p. 160–171, 2024. DOI: <https://doi.org/10.31510/infa.v21i2.2067>. Disponível em: <https://revista.fatectq.edu.br/interfacetecnologica/article/view/2067>. Acesso em: 11 jul. 2026.
- ESNET. **iPerf3**. Versão 3.22. Berkeley: ESnet, 2026. Software de teste de desempenho de rede. Disponível em: <https://iperf.fr>. Acesso em: 16 jul. 2026.
- FERREIRA, Lucas Gabriel Tavares *et al.* Network monitoring using Zabbix, Grafana, and ZeroTier. **Caderno Pedagógico**, Curitiba, v. 22, n. 14, p. 1–32, 2025. DOI: <https://doi.org/10.54033/cadpedv22n14-034>. Disponível em: <https://ojs.studiespublicacoes.com.br/ojs/index.php/cadped/article/view/22081>. Acesso em:

11 jul. 2026.

GRAFANA LABS. **Grafana**. Versão 13.2.4. Nova York: Grafana Labs, 2026. Software de visualização de dados. Disponível em: <https://grafana.com>. Acesso em: 16 jul. 2026.

NETGATE. **pfSense CE**. Versão 2.7.0. Austin: Netgate, 2026. Software de firewall. Disponível em: <https://docs.netgate.com/pfsense/en/latest/releases/2-7-0.html>. Acesso em: 13 jul. 2026.

PROXMOX SERVER SOLUTIONS GMBH. **Proxmox VE**. Versão 8.0.3. Viena: Proxmox Server Solutions GmbH, 2026. Software de virtualização. Disponível em: <https://pve.proxmox.com/pve-docs-8/index.html>. Acesso em: 12 jul. 2026.

SILVA, Carlos Henrique Garcia da. **Monitoramento de ambiente de rede com a ferramenta Zabbix**. Orientador: Helyane Bronoski Borges. 2021. Trabalho de Conclusão de Curso (Tecnólogo em Análise e Desenvolvimento de Sistemas) – Universidade Tecnológica Federal do Paraná, Ponta Grossa, 2021. Disponível em: <http://repositorio.utfpr.edu.br/jspui/handle/1/26453>. Acesso em: 11 jul. 2026.

SILVA, Roger Assunção da; SILVA, Wagner José da. A implementação do Zabbix com segurança: um estudo de caso Zabbix Safely. **Revista Foco**, Curitiba, v. 17, n. 4, p. 1–10, 2024. DOI: <https://doi.org/10.54751/revistafoco.v17n4-055>. Disponível em: <https://ojs.focopublicacoes.com.br/foco/article/view/4851>. Acesso em: 20 abr. 2026.

UBIQUITI INC. **UniFi Network**. Versão 9.0.114. Nova York: Ubiquiti Inc., 2026. Software de gerenciamento de rede. Disponível em: <https://www.ui.com/download/unifi>. Acesso em: 16 jul. 2026.

YIN, R. K. **Estudo de Caso: Planejamento e métodos**. 5. ed. Porto Alegre: Bookman editora, 2015.

ZABBIX SIA. **Zabbix**. Versão 7.0 LTS. Riga: Zabbix SIA, 2026a. Software de monitoramento de redes. Disponível em: <https://www.zabbix.com>. Acesso em: 12 jul. 2026.

ZABBIX SIA. **Zabbix Documentation**. Versão 7.0. Riga: Zabbix SIA, 2026b. Disponível em: <https://www.zabbix.com/documentation/7.0/en/manual>. Acesso em: 13 jul. 2026.