DESTAQUES ACADÊMICOS
UNIVATES | CIÊNCIAS EXATAS E TECNOLÓGICAS
Revista Destaques Acadêmicos, Lajeado, v. 17, n. 4, 2025. ISSN 2176-3070
DOI: https://doi.org/10.22410/issn.2176-3070.v17i4a2025.4291
https://www.univates.br/revistas

MONITORAMENTO DE ATIVOS DE REDE UTILIZANDO FERRAMENTA DE SOFTWARE DE CÓDIGO ABERTO

Diego Guimarães Viana Rodrigues[1], Lucas de Souza Gonçalves[2], Lucas Moreno de Oliveira[3], Plínio Rodrigues Rosa Barreto[4]

Resumo: A crescente complexidade das redes de computadores, aliada à alta dependência de serviços digitais, exige estratégias eficazes para assegurar a disponibilidade, o desempenho e a segurança dos recursos de Tecnologia da Informação e Comunicação (TIC). Nesse contexto, o monitoramento de ativos de rede configura-se como prática essencial para a gestão proativa de ambientes cada vez mais interconectados. Este artigo tem como objetivo a implantação da ferramenta de código aberto Zabbix para o monitoramento de ativos de rede, com vistas a aprimorar a gestão, a segurança e a disponibilidade dos recursos de TIC em um ambiente institucional. A metodologia adotada envolveu revisão bibliográfica sobre conceitos fundamentais de gerenciamento de redes, ferramentas de monitoramento e protocolos, além de levantamento *in loco* dos ativos presentes no laboratório de ensino do Instituto Federal Fluminense *campus* Campos-Centro, seguido da instalação, configuração e personalização do Zabbix. Os resultados indicam a viabilidade e a eficácia da utilização do Zabbix como solução de monitoramento de rede, reforçando o papel de softwares de código aberto como alternativas robustas e economicamente viáveis para instituições de ensino e outras organizações. A documentação do processo e dos parâmetros adotados contribui para a adoção da solução em contextos semelhantes.

Palavras-chave: gerenciamento de redes; ativos de rede; ferramenta de monitoramento; Zabbix; código aberto.

1 Graduando no Curso Superior de Tecnologia em Sistemas de Telecomunicações do Instituto Federal Fluminense *Campus* Campos-Centro, diegoguima2@gmail.com.

2 Graduando no Curso Superior de Tecnologia em Sistemas de Telecomunicações do Instituto Federal Fluminense *Campus* Campos-Centro, lucasgonsouza7@gmail.com.

3 Graduando no Curso Superior de Tecnologia em Sistemas de Telecomunicações do Instituto Federal Fluminense *Campus* Campos-Centro, lucasmorenooliveira9@gmail.com.

4 Professor da área de telecomunicações e membro do Núcleo de Pesquisas em Telecomunicações do IFFluminense, Mestre em Pesquisa Operacional e Inteligência Computacional (UCAM), pbarreto@iff.edu.br.

NETWORK ASSET MONITORING USING OPEN SOURCE SOFTWARE TOOL

Abstract: The growing complexity of computer networks, coupled with their high reliance on digital services, demands effective strategies to ensure the availability, performance, and security of Information and Communication Technology (ICT) resources. In this context, network asset monitoring is an essential practice for the proactive management of increasingly interconnected environments. This article aims to implement the open-source Zabbix tool for network asset monitoring, aiming to improve the management, security, and availability of ICT resources in an institutional environment. The methodology adopted involved a literature review on fundamental network management concepts, monitoring tools, and protocols, as well as an on-site survey of assets located in the teaching laboratory of the Instituto Federal Fluminense Campos-Centro campus, followed by the installation, configuration, and customization of Zabbix. The results indicate the feasibility and effectiveness of using Zabbix as a network monitoring solution, reinforcing the role of open-source software as a robust and economically viable alternative for educational institutions and other organizations. Documenting the process and parameters adopted contributes to the adoption of the solution in similar contexts.

Keywords: network management; network assets; monitoring tool; Zabbix; open source.

1 INTRODUÇÃO

As redes de computadores desempenham um papel central na operação de empresas, instituições e na vida cotidiana das pessoas. A crescente complexidade dessas redes, aliada à dependência de serviços digitais, torna imprescindível a adoção de estratégias eficientes para assegurar a disponibilidade, o desempenho e a segurança dos recursos de Tecnologia da Informação e Comunicação (TIC) (Silva; Santos; Oliveira, 2024).

Nesse cenário, o monitoramento de redes e sistemas emerge como uma prática fundamental para a gestão proativa desses recursos, para garantir a continuidade operacional e a qualidade dos serviços oferecidos pelas organizações. Dessa forma, o monitoramento de ativos de rede desempenha um papel crucial ao possibilitar a detecção precoce de falhas e agilizar a resolução de problemas (De Oliveira *et al.*, 2023).

Este monitoramento consiste na coleta contínua de informações sobre o funcionamento de dispositivos como roteadores, switches, servidores, entre outros ativos, permitindo a identificação de interrupções nos serviços, a otimização de recursos e a tomada de decisões (Barros, 2022).

Para isso, diversas soluções têm sido desenvolvidas, sendo a ferramenta de software de código aberto Zabbix uma das opções mais populares e robustas disponíveis no mercado. Sua capacidade de monitorar uma ampla variedade de dispositivos, gerar alertas em tempo real e produzir relatórios fazem dela uma solução importante para o gerenciamento de redes (Kara; Tuğrul, 2025).

Nesse contexto, a definição de software de código aberto não se restringe, necessariamente, a uma ferramenta disponibilizada sob licença gratuita, pois ela está mais relacionada a uma abordagem de cooperação entre os atores de uma comunidade tecnológica, na qual o código-fonte é acessível e passível de modificação pelo usuário. Desse modo, diversas organizações vêm adotando softwares de código aberto para diferentes finalidades, motivadas por fatores que vão desde a qualidade até considerações orçamentárias (De Oliveira *et al.*, 2023).

Assim sendo, mais de 75% das organizações globais aumentaram o uso de soluções de código aberto em 2022, comparado com anos anteriores (Hughes, 2022). Também, uma pesquisa conduzida pela empresa Tidelift revelou que, em decorrência de fatores relacionados à crise econômica de 2020, cerca de 68% das organizações entrevistadas adotaram essas soluções com o objetivo de reduzir custos.

Complementarmente, dados coletados pela O'Reilly Media em parceria com a IBM indicam que, no segundo semestre de 2020, aproximadamente 94% dos desenvolvedores entrevistados consideraram que as soluções de código aberto eram equivalentes ou superiores aos softwares proprietários, reforçando a crescente confiança e preferência por essa modalidade (Germain, 2021).

Diante desse panorama, este artigo tem como objetivo explorar a utilização da ferramenta de software de código aberto Zabbix para o monitoramento de ativos de rede, por meio de uma abordagem prática que envolveu sua instalação, configuração e personalização, aplicada ao ambiente do laboratório de ensino do Instituto Federal Fluminense *campus* Campos-Centro. A proposta visa contribuir para a melhoria da gestão, da segurança e da disponibilidade dos recursos de TIC. Além disso, são abordados os fundamentos teóricos relacionados ao gerenciamento de redes, às ferramentas de monitoramento e aos protocolos de comunicação comumente utilizados nesse tipo de ambiente.

2 GERENCIAMENTO DE REDES

A importância do gerenciamento de redes, em consonância com a governança de Tecnologias da Informação e Comunicação (TIC), está diretamente relacionada à capacidade de adoção de decisões proativas, com o objetivo de prevenir que falhas comprometam o funcionamento e os objetivos estratégicos da organização (Giamattei *et al.*, 2024).

Nesse sentido, o gerenciamento de redes pode ser estruturado em cinco categorias principais: gestão de falhas, gestão de desempenho, gestão de configuração, gestão de segurança e gestão de contabilização (Hentges; Schorr, 2022).

Dessa forma, problemas relacionados ao congestionamento, latência, perda de pacotes e outras métricas que impactam o desempenho da rede,

são exemplos de como a gestão de desempenho está intrinsecamente ligado à gestão de falhas, uma vez que ambos visam monitorar e controlar a rede de modo a assegurar sua operação com eficiência (Silva; Santos; Oliveira, 2024).

Contudo, um dos principais desafios enfrentados no gerenciamento de redes refere-se à crescente diversidade de dispositivos e softwares de TIC, impulsionada pelo advento de tecnologias, tais como Internet das Coisas (IoT), computação em nuvem e computação móvel (Basso, 2020; Kara; Tuğrul, 2025).

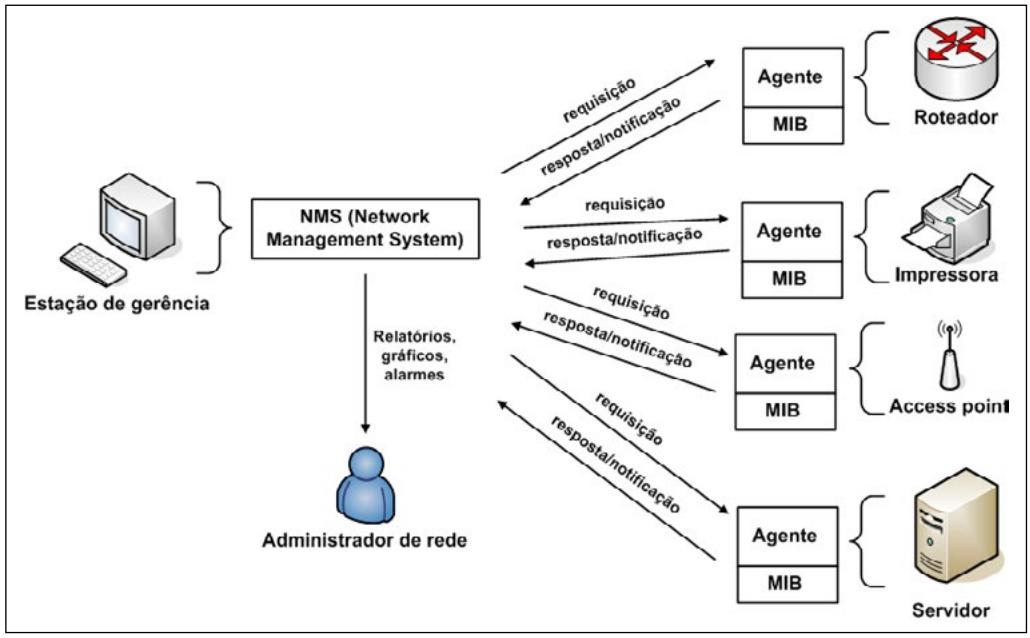
Nessa conjuntura, os sistemas de gerenciamento de redes desempenham funções essenciais, incluindo a coleta de dados e informações gerenciais dos dispositivos, além de oferecerem portabilidade e integrarem-se a outros sistemas de gestão. Esses sistemas também realizam a identificação e organização das informações gerenciais, apresentando-as por meio de recursos como planilhas, gráficos, vetores, relatórios e valores lógicos, dentre outros (Basso, 2020).

Assim, o sistema de gerenciamento de uma rede que conta com diversos equipamentos de TIC de diferentes fabricantes, modelos e propósitos, deve atender às seguintes exigências (Basso, 2020):

- Interface de administração intuitiva, com elementos gráficos de qualidade;
- Portabilidade, sendo compatível com várias plataformas (Windows, Linux e outros sistemas operacionais);
- Variedade de gráficos e relatórios para apoiar a tomada de decisões;
- Disponibilidade de módulos extras para auditoria, registro de problemas, inventário, monitoramento de disponibilidade, capacidade, configuração e desempenho.

Ademais, a arquitetura de um sistema de gerenciamento de rede geralmente segue uma estrutura básica composta por três componentes principais: entidade gerenciadora, dispositivos gerenciados e protocolos de gerenciamento de rede (Silva; Santos; Oliveira, 2024). A Figura 1 apresenta uma visão geral da arquitetura de um sistema de gerenciamento.

Figura 1 - Visão geral da arquitetura gerente-agente



Fonte: DevMedia (2025).

Adicionalmente, Basso (2020) destaca os elementos que o sistema de gerenciamento de rede deve incluir:

- Banco de dados para armazenar informações;
- Agentes e gerentes para monitoramento;
- Gerenciador de relatórios;
- Mapas e visualizações da rede;
- Modelos de gerenciamento (*templates*).

A entidade gerenciadora é responsável pelo controle e supervisão dos dispositivos e recursos da rede. Ela pode ser implementada como uma ferramenta de software ou um sistema dedicado, desempenhando diversas funções relacionadas ao gerenciamento da rede. Essa entidade atua como um centro de controle, encarregada de coletar, processar, analisar e apresentar informações de gerenciamento de rede, garantindo uma visão integrada do funcionamento da infraestrutura. A estação de gerenciamento de rede (NMS - *Network Management System*) é o servidor onde o software de gerenciamento de rede está instalado.

Os dispositivos gerenciáveis em redes de computadores referem-se àqueles que possuem um endereço IP na rede e que contam com um agente de gerenciamento instalado. Este agente estabelece conexão com a entidade

gerenciadora e realiza ações específicas nos dispositivos sob sua supervisão, de acordo com as instruções recebidas, facilitando o monitoramento remoto.

Por fim, os protocolos de gerenciamento são utilizados para a troca de informações entre a estação de gerenciamento e os agentes presentes nos dispositivos de rede. Esses protocolos garantem a comunicação eficiente e segura, permitindo a implementação de políticas de gerenciamento e a coleta de dados essenciais para a manutenção e otimização da rede (Kara; Tuğrul, 2025).

2.1 Protocolos utilizados

Os protocolos são cruciais para a comunicação entre dispositivos conectados à rede de computadores, estabelecendo um conjunto de diretrizes que viabilizam a troca de informações entre equipamentos de diferentes fabricantes e sistemas operacionais.

O protocolo de mensagens de controle da internet (ICMP - *Internet Control Message Protocol*), por exemplo, é um protocolo de comunicação que opera na camada de rede (camada 3) do modelo OSI. Sua principal função consiste em fornecer informações de controle e gerenciamento relacionadas à comunicação de rede.

Conjuntamente, o protocolo de gerenciamento de rede simples (SNMP - *Simple Network Management Protocol*) é amplamente utilizado no gerenciamento de redes, permitindo que os administradores monitorem o desempenho da rede, coletem informações de gerenciamento e detectem falhas em uma variedade de dispositivos de diferentes fabricantes, como roteadores, switches, impressoras, firewalls, servidores, dentre outros.

As informações gerenciais de cada dispositivo são armazenadas em bases de informações de gerenciamento (MIB - *Management Information Base*), as quais são integradas aos agentes nos dispositivos gerenciados, possibilitando a coleta, armazenamento e troca de dados para a administração da redes (Silva; Santos; Oliveira, 2024; Kara; Tuğrul, 2025).

2.2 Ferramentas de monitoramento

Atualmente, observa-se uma variedade de ferramentas de monitoramento de rede, as quais podem ser classificadas em soluções pagas e gratuitas, cada uma apresentando distintas vantagens e limitações. Dessa forma, a diversidade de produtos e soluções disponíveis no mercado resulta em ferramentas que diferem significativamente em termos de complexidade, funcionalidades e estratégias de implementação. Além disso, a seleção da ferramenta mais adequada para uma organização deve considerar suas necessidades específicas, uma vez que uma solução eficaz para uma instituição pode não ser apropriada para outra.

Portanto, ferramentas de monitoramento de rede têm como objetivo principal a coleta de dados referentes ao status de ativos e softwares em sistemas de informação e comunicação, possibilitando a detecção de falhas, análise de desempenho e manutenção preditiva. Exemplos utilizados na prática incluem Cacti, IBM Tivoli, Nagios, Open NMS, Prometheus, SolarWinds, Zabbix, dentre outros (Barros, 2022; Kara; Tuğrul, 2025). O Quadro 1 elenca as características de algumas dessas ferramentas.

Quadro 1 – Características das ferramentas de monitoramento

Ferramenta de Monitoramento	**Características**	**Código aberto**	**Classificação**
Cacti	Recursos avançados de automação baseados em modelos para dispositivos, gráficos e árvores, vários métodos de aquisição de dados, capacidade de ser estendido por meio de *plug-ins*, recursos de gerenciamento de usuários, grupos e domínios baseados em funções, além de um mecanismo de criação de temas e suporte a vários idiomas.	Sim	Gratuita
IBM Tivoli	Projetada para administrar ambientes de grande escala, incluindo *data centers* complexos e infraestruturas de nuvem, com funcionalidades como automação de tarefas, monitoramento de recursos, gerenciamento de mudanças e configurações, além de ferramentas voltadas para a análise e otimização do desempenho do sistema.	Não	Paga
Nagios	Capacidade de gerenciar ambientes complexos e implantações em larga escala, permitindo o monitoramento integrado de aplicativos, serviços, sistemas operacionais, protocolos de rede, métricas de sistema e componentes de infraestrutura, tudo por meio de uma única ferramenta.	Sim	Gratuita
OpenNMS	Funcionalidades que abrangem a supervisão detalhada do status e do desempenho de ativos de rede, servidores, máquinas virtuais e serviços. A plataforma permite a visualização e o monitoramento integrado de redes locais e distribuídas, proporcionando uma abordagem abrangente para a detecção de falhas, análise de desempenho, monitoramento de tráfego e geração de alertas.	Sim	Gratuita / Paga
Prometheus	Ferramentas de monitoramento e alerta de sistemas, que coleta e armazena suas métricas como dados de séries temporais, ou seja, as informações das métricas são armazenadas com o registro de data e hora em que foram registradas, juntamente com pares de chave-valor opcionais chamados rótulos.	Sim	Gratuita

Ferramenta de Monitoramento	Características	Código aberto	Classificação
SolarWinds	Fornece recursos essenciais para o monitoramento eficiente, incluindo mapeamento de rede, servidores *syslog*, interceptação de SNMP e instrumentos de sondagem de dispositivos universais, além de alertas avançados configuráveis e funcionalidades para a criação e o envio de relatórios.	Não	Paga
Zabbix	Robustez, flexibilidade e capacidade de monitoramento abrangente, possibilita a coleta de dados de uma variedade de ativos de rede, incluindo servidores, switches, roteadores, bem como máquinas virtuais e serviços em nuvem.	Sim	Gratuita

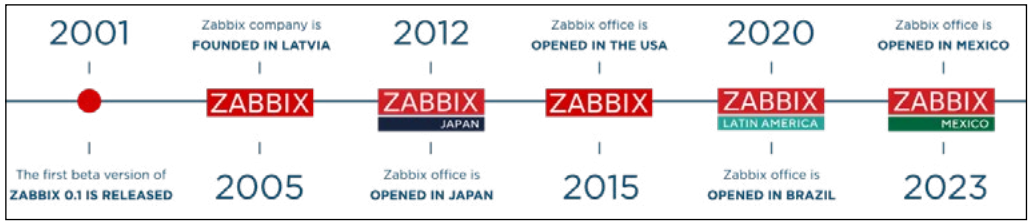
Fonte: Adaptado de Kara e Tuğrul (2025).

De acordo com estudos relacionados à longevidade de softwares, observa-se que ferramentas proprietárias tendem a apresentar maior estabilidade, embora existam exceções, como o Zabbix e o Nagios, ambos de código aberto, gratuitas e com mais de 20 anos de existência no mercado (Giamattei *et al.*, 2024).

2.2.1 Zabbix

O Zabbix constitui uma ferramenta de software de código aberto voltada ao monitoramento de redes de computadores, desenvolvida e apoiada pela empresa Zabbix LLC, fundada há mais de 20 anos, por Alexei Vladishev. A companhia, sediada na Letônia, abriu escritórios em vários países ao longo dos anos, conforme pode ser observado na Figura 2.

Figura 2 – Evolução da companhia Zabbix LLC



Fonte: Zabbix (2025).

Trata-se de uma solução de monitoramento capaz de acompanhar a saúde e a integridade de diversos componentes de infraestrutura de TIC, incluindo ativos de rede, servidores, máquinas virtuais, aplicações, serviços, bancos de dados, sites e ambientes em nuvem.

A plataforma dispõe de um sistema de notificações versátil, que possibilita o envio de alertas por e-mail e/ou aplicativo de mensagem

instantânea, para sinalizar uma gama de eventos, promovendo respostas ágeis frente a incidentes operacionais.

Ademais, o Zabbix oferece recursos avançados para geração de relatórios e visualização de dados baseados nos registros coletados, incorpora recursos de automação destinados à simplificação das tarefas rotineiras e oferece escalabilidade compatível com ambientes que demandam monitoramento em larga escala o que o se destaca como uma das ferramentas mais poderosas e flexíveis para o monitoramento de redes de computadores da atualidade (Barros, 2022; Silva; Silva, 2024).

2.2.1.1 Arquitetura e componentes do Zabbix

A arquitetura do Zabbix pode ser caracterizada como um sistema de monitoramento semi-distribuído com gerência centralizada. Em determinadas implantações, observa-se o uso de um banco de dados central para o armazenamento de séries temporais, eventos e metadados.

Em outras configurações, é viável empregar uma topologia de monitoramento distribuído, na qual nós coletam dados localmente e comunicam-se com um servidor *proxy* para agregação e encaminhamento ao servidor central (Valente, 2023; Guo; Chen; Li, 2024; Silva; Santos; Oliveira, 2024).

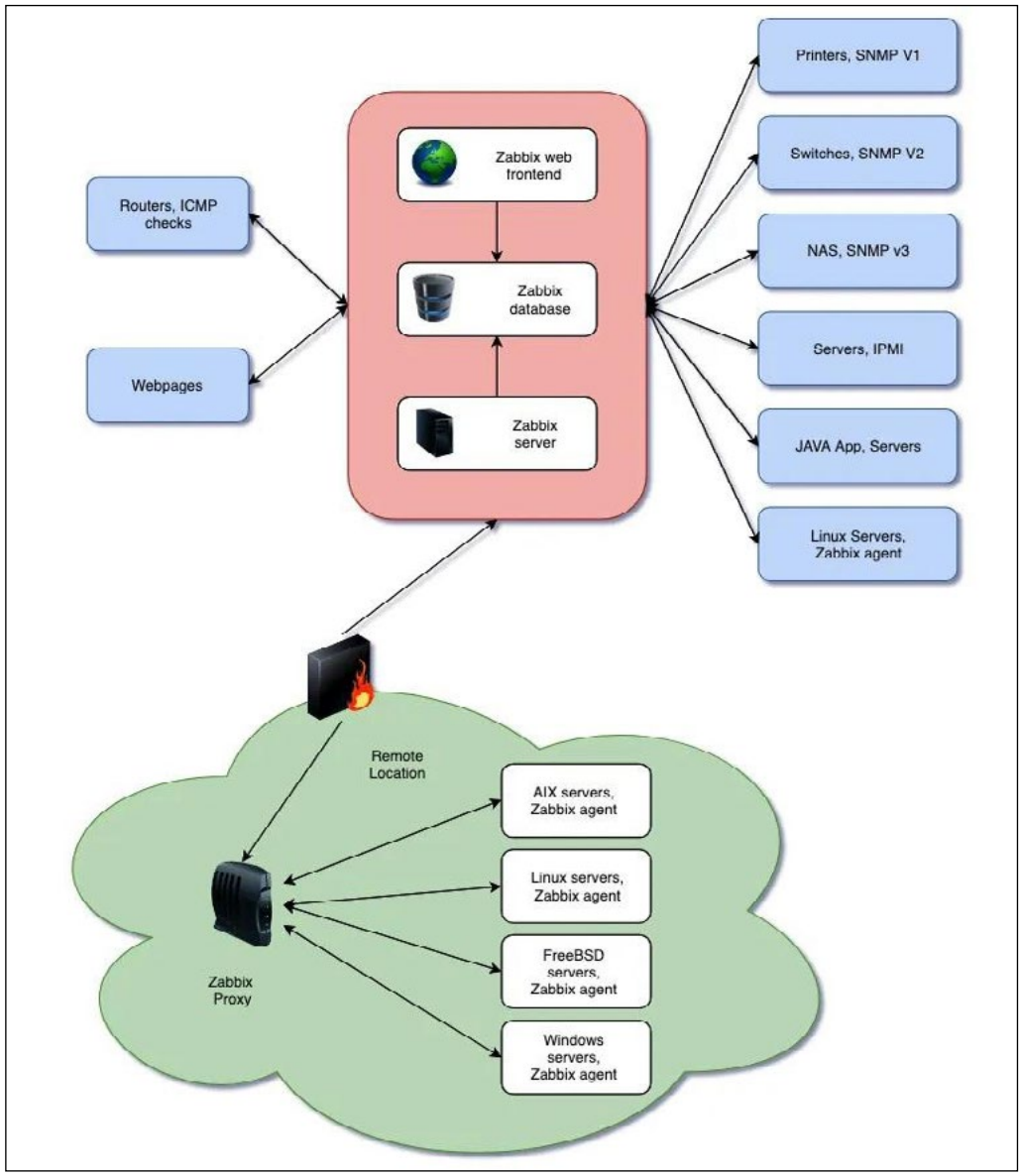
De acordo com a documentação oficial disponível no *website* da ferramenta, o Zabbix adota uma arquitetura composta por diferentes componentes de software, cujas funcionalidades são descritas a seguir:

- Servidor Zabbix (*Zabbix Server*): componente central para quem os agentes reportam informação de disponibilidade e integridade, bem como estatísticas;
- Banco de Dados (*Zabbix Database*): um repositório central, onde todas as configurações, informações estatísticas e operacionais são armazenadas;
- Interface Web (*Zabbix Web Frontend*): para simplificar o acesso ao Zabbix de qualquer lugar e de qualquer plataforma, é disponibilizada de forma nativa uma interface web, que normalmente (mas não necessariamente) roda na mesma máquina física que o servidor Zabbix;
- *Zabbix Proxy* (opcional): coleta informação de disponibilidade e desempenho como se fosse o servidor Zabbix, passando para este, em momento oportuno, as informações coletadas, para distribuição de carga em relação a uma arquitetura com apenas um servidor central;
- Agente Zabbix *(Zabbix Agent):* são implantados diretamente nas máquinas alvo, para monitorar recursos locais (memória,

processador, discos, usuários, interface de rede, dentre outros) e aplicações, reportando a informação coletada ao servidor Zabbix.

A Figura 3 ilustra a arquitetura convencional em um sistema de monitoramento Zabbix, relativamente comum, mas que possibilita ampla capacidade de monitoramento em uma rede composta por equipamentos e dispositivos variados.

Figura 3 – Arquitetura convencional de monitoramento Zabbix



Fonte: Adaptado de Aguiar (2017).

3 METODOLOGIA

Este estudo adotou uma abordagem predominantemente descritiva, de natureza aplicada e com objetivo exploratório. Para atingir o objetivo proposto, foram delineadas três etapas principais, descritas a seguir.

A primeira etapa consistiu na pesquisa bibliográfica, cujo propósito foi aprofundar o entendimento dos conceitos fundamentais relacionados ao tema do trabalho. Foram investigados conceitos de gerenciamento de redes, ferramentas de monitoramento e protocolos de comunicação envolvidos. A pesquisa foi realizada por meio da consulta a trabalhos acadêmicos disponíveis nas plataformas Scielo e Google Acadêmico, bem como em periódicos científicos relevantes indexados nas bases Scopus e Web of Science. Essa etapa permitiu consolidar o embasamento teórico necessário para o desenvolvimento das etapas subsequentes do trabalho.

A segunda etapa consistiu na realização de um levantamento *in loco* dos equipamentos ativos presentes no laboratório de ensino de cabeamento estruturado e redes de computadores do *campus* Campos-Centro do Instituto Federal Fluminense. Este laboratório simula as instalações de um edifício comercial de três pavimentos. Durante essa fase, foram identificados e catalogados os dispositivos ativos disponíveis, com o objetivo de verificar a compatibilidade e a adequação desses às funcionalidades e recursos oferecidos pela ferramenta de monitoramento Zabbix.

A terceira e última etapa envolveu a instalação, configuração e personalização do ambiente de monitoramento, adaptando-o às necessidades específicas da rede em questão. Este procedimento incluiu a implementação do Zabbix, bem como a definição de métricas e *templates* adequados para o monitoramento dos ativos identificados na etapa anterior. Além disso, foram documentadas todas as etapas do processo de implantação, incluindo configurações realizadas e ajustes efetuados. Os resultados obtidos durante essa fase foram registrados para subsidiar a análise subsequente da eficácia do sistema de monitoramento implantado.

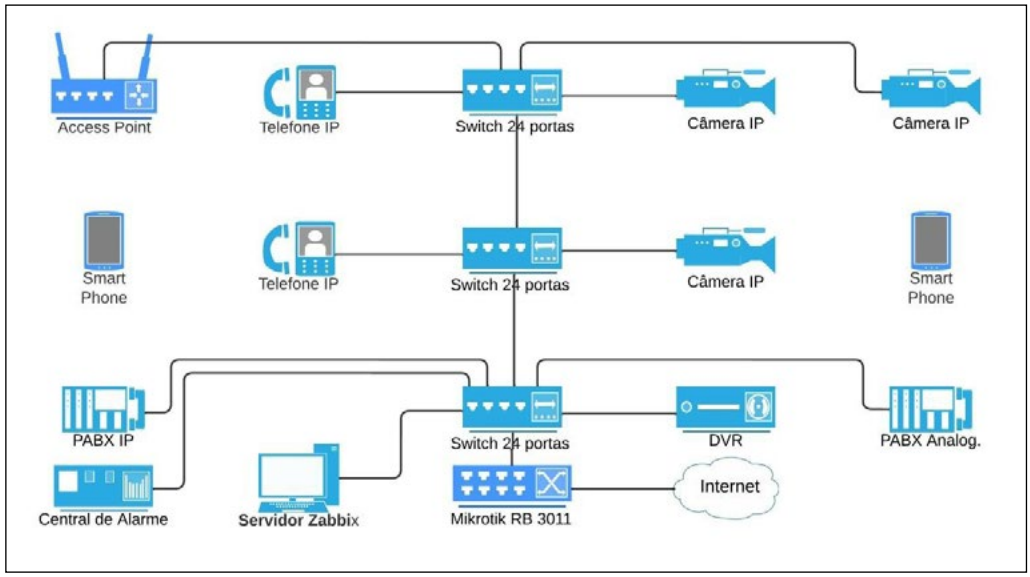
4 RESULTADOS

4.1 Descrição do ambiente

A partir do levantamento *in loco* realizado no laboratório de ensino de cabeamento estruturado e redes de computadores do *campus* Campos-Centro do Instituto Federal Fluminense, identificou-se uma diversidade de equipamentos ativos de rede, devidamente organizados conforme a disposição apresentada na Figura 4.

Nessa ocasião, foram coletados dados relevantes dos ativos de rede, tais como fabricante, modelo, localização física e endereço IP. As informações obtidas foram consolidadas no Quadro 2.

Figura 4 – Disposição dos equipamentos ativos de rede



Fonte: Elaboração própria (2025).

Quadro 2 – Dados e características dos ativos de rede

Dispositivo	Fabricante	Modelo	Localização	Endereço IP
Roteador 10 portas gigabit ethernet	MikroTik	RB3011UiAS	Sala de equipamentos do pavimento térreo	192.168.88.101
Switch 24 portas gigabit ethernet	HPE	OfficeConnect Switch 1920S 24G 2SFP JL381A	Sala de equipamentos do pavimento térreo	192.168.88.102
Switch 24 portas gigabit ethernet	HPE	OfficeConnect Switch 1920S 24G 2SFP JL381A	Sala de telecomunicações do 1º andar	192.168.88.103
Switch 24 portas fast ethernet	3Com	3CR17333A-9	Sala de telecomunicações do 2º andar	192.168.88.104
Central de alarme	Intelbras	AMN 24 NET	Sala de equipamentos do pavimento térreo	192.168.88.105
Central telefônica PABX	Intelbras	Impacta 40	Sala de equipamentos do pavimento térreo	192.168.88.106

Dispositivo	Fabricante	Modelo	Localização	Endereço IP
DVR 16 canais	Intelbras	MHDX 5016	Sala de equipamentos do pavimento térreo	192.168.88.107
Câmera IP 01	Hikvision	DS-2CD1323G0E-I	Área de trabalho do 2º andar	192.168.88.108
Câmera IP 02	Hikvision	DS-2CD1323G0E-I	Área de trabalho do 2º andar	192.168.88.109
Access Point	TP-Link	Archer C50	Área de trabalho do 2º andar	192.168.88.110
Telefone IP	Intelbras	TIP 125	Área de trabalho do 1º andar	192.168.88.111
Câmera IP 03	Hikvision	DS-2CD1323G0E-I	Área de trabalho do 1º andar	192.168.88.112
Telefone IP	Yealink	SIP-T22P	Área de trabalho do 2º andar	192.168.88.113
Central telefônica IP	FreePBX	Raspberry pi 3	Sala de equipamentos do pavimento térreo	192.168.88.114

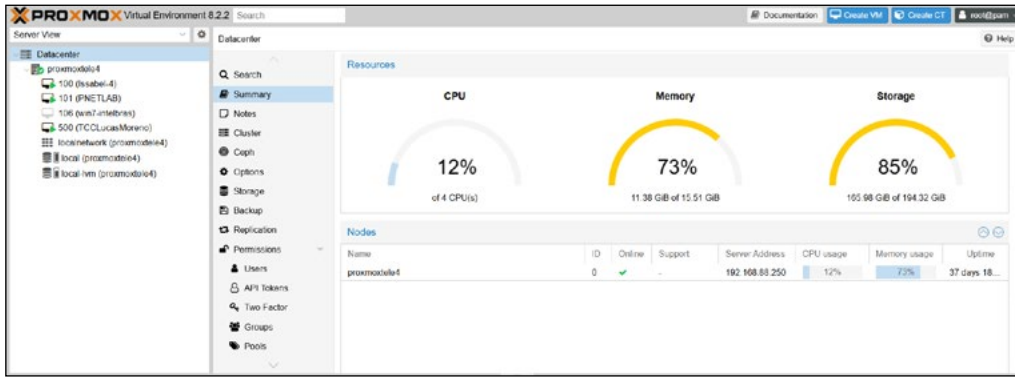
Fonte: Elaboração própria (2025).

4.2 Instalação e configuração da ferramenta

A instalação do servidor Zabbix requer atendimentos a requisitos mínimos de memória e armazenamento. De acordo com as especificações oficiais, recomenda-se memória RAM de 128 Megabytes (MB) e armazenamento em disco de 256 MB. Contudo, a demanda efetiva por esses recursos é dependente do número de *hosts* monitorados e das métricas acompanhadas pela ferramenta, aumentando conforme a escala da implantação. Além disso, recomenda-se reservar espaço adicional em disco para assegurar a disponibilidade adequada do banco de dados em cenários que exijam a manutenção de um histórico prolongado das métricas monitoradas (Zabbix, 2025).

A partir da presente exigência e da indisponibilidade de uma máquina física dedicada à ferramenta de monitoramento, o servidor Zabbix foi instalado em uma máquina virtual. Esta máquina está situada em um servidor físico local contendo 4 unidades de processamento, memória RAM de 16 Gigabytes (GB) e disco rígido de 200 GB, com a plataforma de virtualização Proxmox VE 8.2.2 instalada sobre um sistema operacional base Linux Debian, conforme pode ser observado na Figura 5.

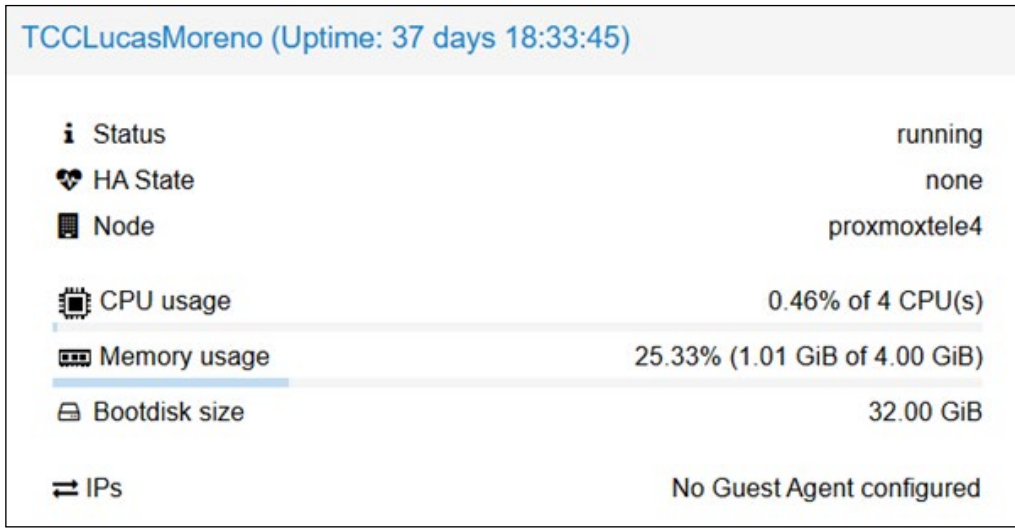
Figura 5 – Configurações do servidor Proxmox Linux



Fonte: Elaboração própria (2025).

Subsequentemente, a versão 7.4 do Zabbix em inglês, disponível no portal oficial, foi implementada na máquina virtual configurada com 4 GB de memória RAM e 32 GB de armazenamento dinamicamente alocado em disco. O sistema operacional instalado nessa máquina virtual foi o Linux Debian versão 12.11 de 64 bits. A Figura 6 apresenta algumas informações referentes à máquina virtual criada.

Figura 6 – Resumo das configurações da máquina virtual

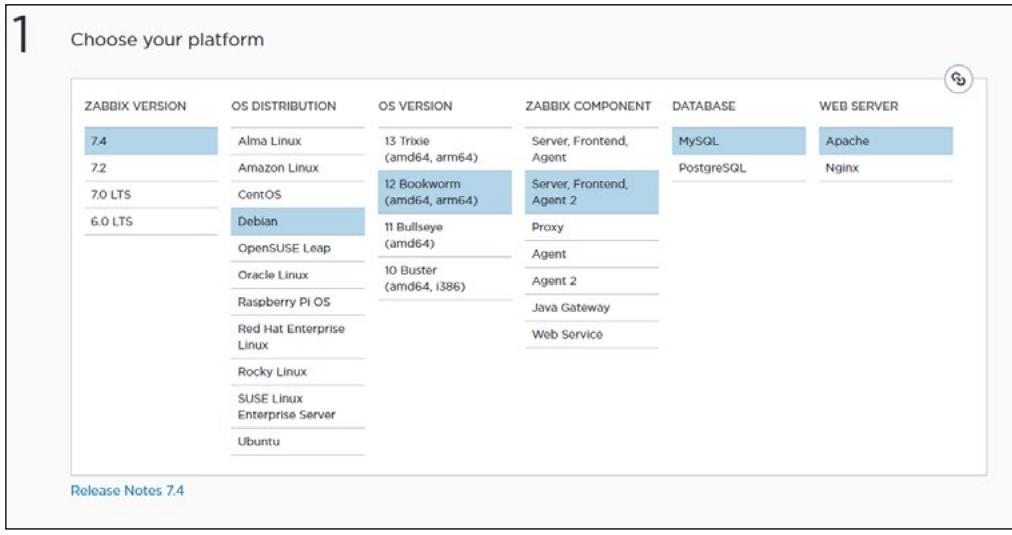


Fonte: Elaboração própria (2025).

4.2.1 Instalação do servidor Zabbix

Como procedimento inicial de instalação, foram obtidos, no site oficial da ferramenta de monitoramento, os comandos necessários para a implantação do servidor *backend* do Zabbix e de seu banco de dados. O próprio site disponibiliza uma interface para a seleção de diretrizes, como versão do Zabbix, sistema operacional, tipo de banco de dados e servidor web a serem utilizados, gerando um *script*, que consiste em um conjunto de instruções personalizadas para o ambiente em questão. A Figura 7 ilustra a etapa de seleção dessas diretrizes para geração do *script*.

Figura 7 – Seleção de diretrizes para geração do *script* de instalação do Zabbix



Fonte: Elaboração própria (2025).

Os comandos disponibilizados foram executados manualmente no terminal do servidor, permitindo que o administrador adaptasse credenciais e configurações conforme os dados desejados. O processo contemplou a instalação dos pacotes essenciais, a configuração inicial do banco de dados, a criação das tabelas necessárias para o funcionamento do sistema e a aplicação das permissões adequadas para comunicação entre o servidor Zabbix e o banco de dados.

Ao término da execução dos comandos, o terminal apresentou o status detalhado de cada etapa realizada, permitindo ao administrador verificar se todas as operações foram concluídas com êxito. Essa validação é essencial para garantir a integridade da instalação e evitar inconsistências que possam comprometer o funcionamento do sistema.

Somente após a confirmação de que todas as etapas foram finalizadas corretamente, prosseguiu-se para a configuração da interface web. Dessa forma, assegura-se que o ambiente de monitoramento esteja completamente preparado para iniciar a coleta de dados e para possibilitar a administração eficiente da infraestrutura monitorada.

4.2.1.1 Configuração da interface web

Com a instalação do pacote da interface web na etapa anterior, deu-se continuidade à configuração diretamente pelo navegador, a qual permitiu a verificação dos pré-requisitos necessários ao funcionamento da interface web do servidor de monitoramento.

Nesta etapa, o sistema realiza uma checagem de compatibilidade para os pacotes, permissões e extensões exigidas pelo Zabbix, verificando a correta instalação e operação. Caso algum componente esteja ausente ou inadequadamente configurado, é emitido um alerta para que o administrator realize os ajustes necessários antes de prosseguir.

Em seguida, realizou-se a configuração dos parâmetros de conexão com o banco de dados do sistema, na qual foram fornecidas as credenciais de acesso: endereço do servidor, nome do banco de dados, usuário e senha, de acordo com o ilustrado na Figura 8.

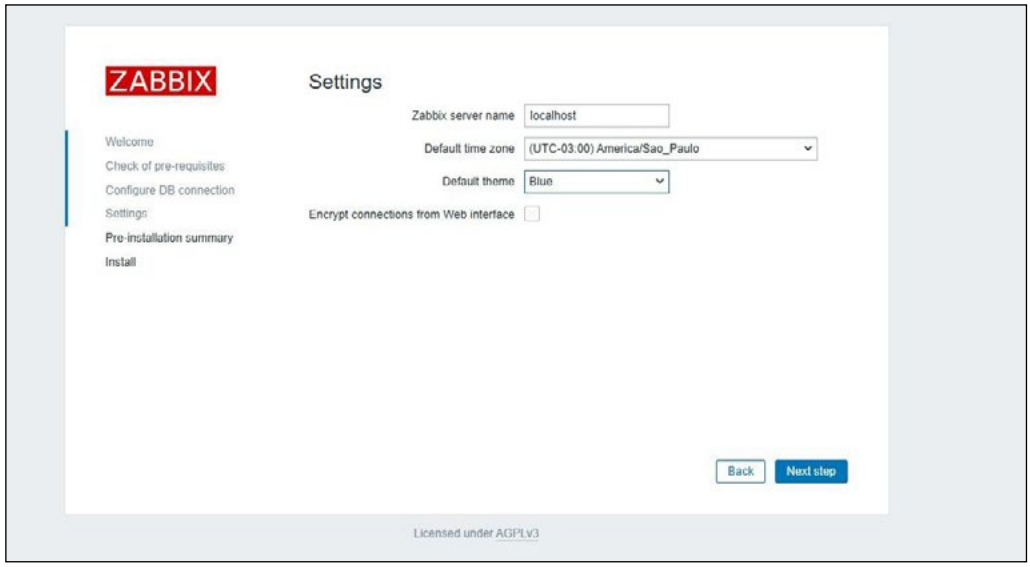
Esta etapa assegura a comunicação adequada entre a interface web e a base de dados que armazena as informações de monitoramento. Destaca-se que, para a conclusão bem-sucedida deste procedimento, a base de dados deve ter sido previamente criada, conforme descrito na etapa anterior, e o servidor MySQL deve estar ativo.

A etapa subsequente consistiu na configuração dos parâmetros do servidor web. Foi definido o nome do servidor, o fuso horário a ser utilizado e o tema ou esquema de cores da interface, conforme apresentado na Figura 9. Essas opções visam aprimorar a interface para melhorar a experiência do usuário.

Figura 8 – Configuração dos parâmetros para conexão com o banco de dados

Fonte: Elaboração própria (2025).

Figura 9 – Configuração dos parâmetros do servidor web



Fonte: Elaboração própria (2025).

Finalmente, foi apresentado um sumário das configurações realizadas para conferência. Ao confirmar a exatidão dos dados e selecionar a opção *Next step*, foi apresentada a tela de confirmação do processo de instalação. E ao selecionar *Finish*, foi exibida a tela de login do Zabbix. O nome do usuário para o acesso inicial ao sistema é definido como "Admin", com a senha padrão "Zabbix".

4.2.2 Configuração do monitoramento do Zabbix

Após a conclusão da configuração da interface web, o sistema torna-se acessível por meio do navegador, possibilitando a operacionalização da configuração e a personalização do ambiente de monitoramento.

Em seguida, ao efetuar o login com credenciais de usuário, foi obtido acesso ao painel de controle e à gestão da ferramenta (*dashboard*). Este painel será apresentado adiante na Figura 13, a qual exibe informações do sistema, passíveis de ajuste conforme as preferências do usuário, por meio dos menus laterais, que fornecem acesso rápido às diferentes áreas de configuração e administração do sistema. Ao selecionar uma das opções, os submenus são expandidos, revelando opções adicionais de configuração com detalhes de gerenciamento.

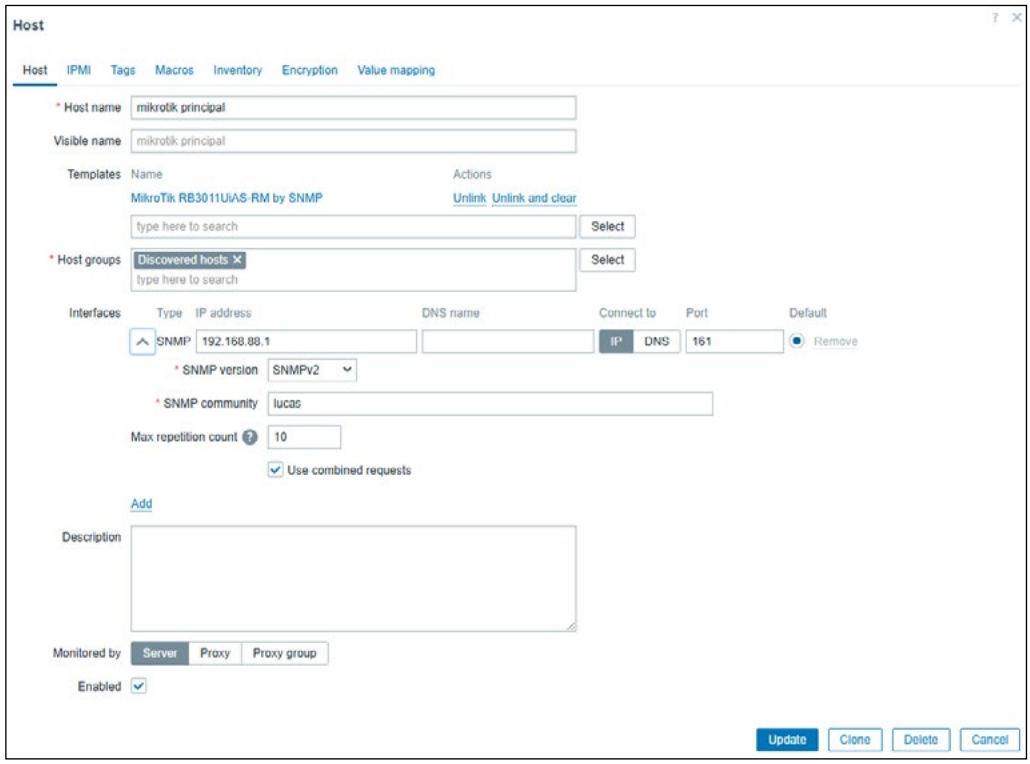
4.2.2.1 Adição de hosts

O *host* constitui um dos elementos centrais da plataforma de monitoramento, representando qualquer dispositivo, serviço ou recurso objeto da observação. Podem incluir-se, entre outros, servidores, switches, roteadores, câmeras IP, telefones IP e aplicações específicas.

Cada *host* é configurado com um endereço IP ou um nome DNS e pode englobar múltiplas interfaces de monitoramento, como agente Zabbix, via SNMP ou via ICMP, conforme a necessidade de coleta de dados. Dessa forma, o cadastro correto dos *hosts* é essencial para garantir que as informações coletadas sejam precisas e que o sistema consiga gerar alertas em tempo hábil diante de falhas ou degradação de desempenho.

Nesse contexto, a Figura 10 exibe a configuração de adição de *host* relativo ao roteador MikroTik RB3011UiAS no sistema Zabbix. Nesta etapa, foram definidos parâmetros fundamentais, incluindo o nome do dispositivo, o grupo de *hosts* ao qual pertence, o endereço IP, a interface de monitoramento (SNMPv2) e a comunidade SNMP utilizada para definição dos status permitidos para o monitoramento. Os demais campos disponíveis que não foram aplicáveis ao cenário proposto permaneceram com a configuração padrão (*default*).

Figura 10 – Configuração de adição de *host* referente ao roteador MikroTik



Fonte: Elaboração própria (2025).

A definição correta desses atributos é crucial, pois assegura que o servidor Zabbix possa identificar e comunicar-se com o roteador de modo contínuo e confiável. Além disso, a vinculação do *host* a um grupo específico favorece a organização lógica da infraestrutura monitorada, facilitando tanto a administração quanto a aplicação de políticas de monitoramento.

De forma semelhante, os demais ativos da rede foram incorporados ao sistema de monitoramento utilizando a interface de ICMP. Essa abordagem permite a obtenção de visibilidade em tempo real do estado dos *hosts*, viabilizando a detecção imediata de falhas de comunicação ou de indisponibilidade, o que reduz o tempo de resposta na solução de problemas e aumenta a confiabilidade dos serviços.

Foram estabelecidos grupos de *hosts* distintos para: switches e *access point*; gravador digital de imagens (DVR) e câmeras IP; central telefônica PABX e telefones IP. A divisão e a atribuição dos *hosts* aos respectivos grupos favorecem a organização do ambiente monitorado, facilitam a administração da infraestrutura e otimizam a análise de incidentes. Em termos de monitoramento, o arranjo promove um monitoramento estruturado dos serviços de voz, dados

e imagem, assegurando que falhas sejam detectadas e tratadas de forma rápida, com consequente minimização dos impactos na operação da rede.

Após a finalização do processo de adição dos *hosts* na plataforma Zabbix, os dispositivos passaram a ser monitorados conforme os parâmetros previamente configurados no sistema. No entanto, observou-se que o correto funcionamento do monitoramento está diretamente condicionado à configuração adequada do agente Zabbix ou do protocolo de comunicação adotado (por exemplo, SNMP ou ICMP) nos respectivos *hosts*. A ausência ou má configuração desses componentes compromete a coleta de dados, prejudicando a efetividade do monitoramento e, consequentemente, a confiabilidade dos resultados obtidos pela ferramenta.

4.2.2.2 Associação de templates aos hosts

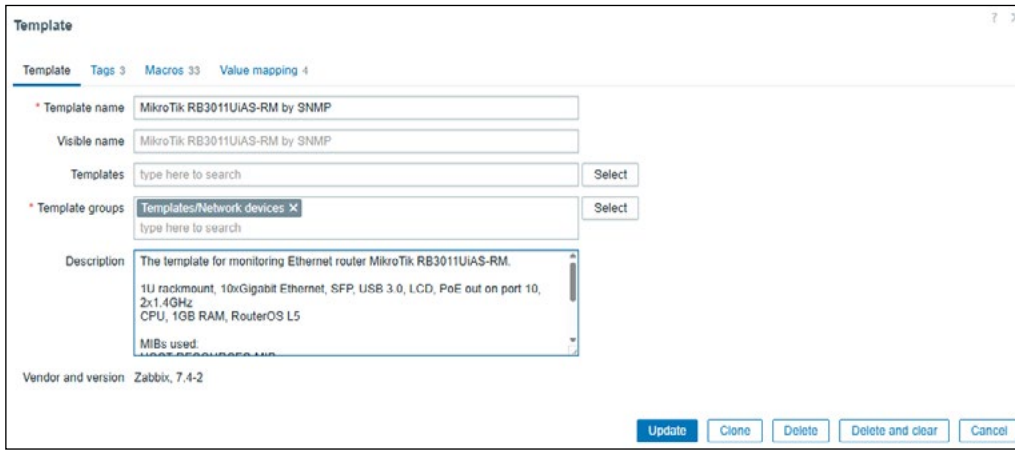
Dando continuidade à configuração dos *hosts* na plataforma Zabbix, a etapa seguinte consistiu na associação de *templates* previamente definidos. Os *templates* são conjuntos estruturados de itens de coleta, configuração de alertas (*triggers*), gráficos e demais elementos de monitoramento, que podem ser reutilizados em diferentes dispositivos. Essa abordagem visa padronizar e agilizar o processo de configuração, eliminando a necessidade de definir individualmente os parâmetros de monitoramento para cada *host*.

Ao associar um *template* a um *host*, este passa automaticamente a herdar todas as configurações contidas no *template*. Dessa forma, o *host* é monitorado com base nas regras e parâmetros já consolidados, permitindo uma gestão centralizada e eficiente. Alterações realizadas no *template* são refletidas em todos os *hosts* vinculados a ele, o que facilita tanto a manutenção quanto a personalização em larga escala, sobretudo em ambientes com grande número de dispositivos monitorados.

Nessa conjuntura, conforme demonstra a Figura 11, foi realizada a associação do *template* baseado no protocolo SNMP ao *host* correspondente ao roteador MikroTik RB3011UiAS. A utilização desse *template* viabilizou a coleta automática de diversos parâmetros operacionais do dispositivo, incluindo o tráfego de rede por interface, utilização de CPU, consumo de memória e verificação de disponibilidade.

O protocolo SNMP é amplamente consolidado em soluções de monitoramento de redes, por permitir uma padronização na coleta de métricas e assegurar interoperabilidade entre equipamentos de diferentes fabricantes. No contexto do Zabbix, a adoção de *templates* baseados em SNMP contribui significativamente para a redução de erros manuais durante a criação de itens, *triggers* e demais elementos de monitoramento, ao mesmo tempo em que favorece a implementação de um monitoramento mais abrangente e preciso.

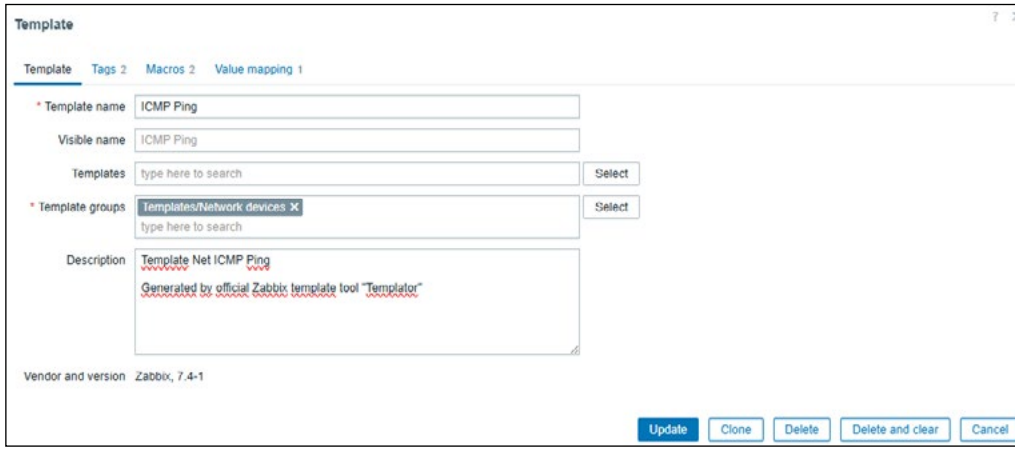
Figura 11 – Associação do *template* ao roteador MikroTik RB3011UiAS



Fonte: Elaboração própria (2025).

Analogamente, a Figura 12 apresenta a configuração do *template* ICMP *Ping* na plataforma Zabbix. Esse *template* é utilizado para o monitoramento da disponibilidade de ativos de rede por meio do protocolo ICMP, permitindo a obtenção de métricas fundamentais como tempo de resposta e taxa de perda de pacotes.

Figura 12 – Associação do *template* aos *hosts* monitorados via ICMP



Fonte: Elaboração própria (2025).

Portanto, o *template* ICMP *Ping* foi associado a todos os *hosts* monitorados exclusivamente via ICMP, abrangendo dispositivos como switches, *access point*, câmeras IP, DVR, central telefônica PABX e telefones IP. Essa abordagem padronizada permite verificar, de forma contínua, a conectividade e

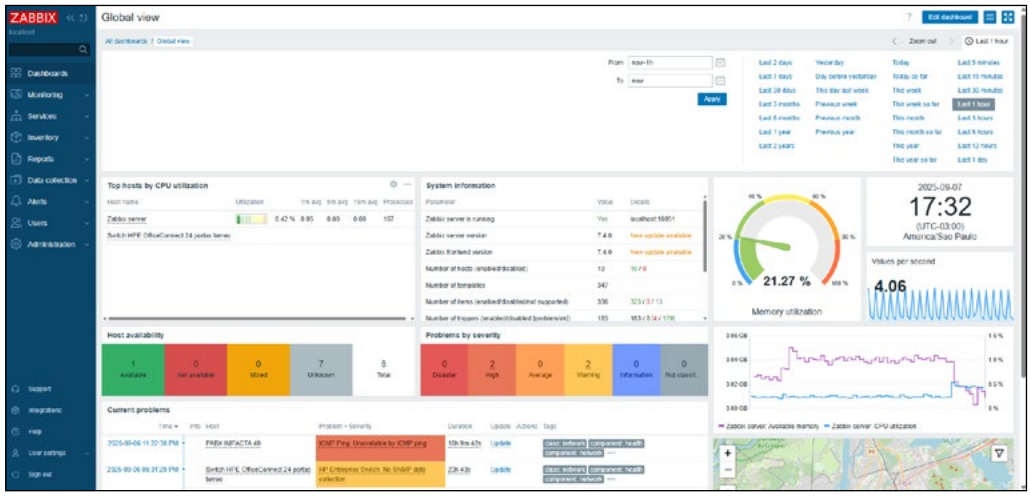
disponibilidade básica dos equipamentos, mesmo na ausência de agentes específicos ou suporte a protocolos mais avançados, como SNMP.

Cabe destacar que, durante a associação dos *templates*, as abas *Tags*, *Macros* e *Value mapping* foram mantidas com suas configurações *default*, tanto para os *hosts* monitorados via protocolo SNMP quanto via ICMP. No entanto, essas seções disponibilizam recursos avançados de configuração que podem ser explorados conforme as particularidades e exigências do ambiente monitorado.

4.3 Visualização dos dados do monitoramento via interface web

Ao acessar a interface web da ferramenta de monitoramento, após o login, foi possível visualizar o *dashboard* do Zabbix (Figura 13). Esse painel fornece uma visão centralizada do ambiente, permitindo identificar rapidamente o estado dos dispositivos e serviços críticos, pois consolida os principais indicadores de desempenho e disponibilidade da infraestrutura monitorada.

Figura 13 – *Dashboard* da interface web do Zabbix



Fonte: Elaboração própria (2025).

Ainda no *dashboard*, a seção *Top hosts by CPU utilization*, exibe o consumo de processamento do servidor Zabbix e do switch HPE OfficeConnect 24 portas. Observa-se que o servidor Zabbix apresenta baixa utilização de CPU (0,42%), indicando que os recursos computacionais estão sendo consumidos de forma estável e sem sobrecarga. Esse tipo de métrica é fundamental para avaliar a saúde do servidor de monitoramento e garantir que ele possua capacidade suficiente para processar os dados coletados.

Já no quadro *System information*, são listadas informações relevantes sobre o ambiente, como a versão do servidor e *frontend* do Zabbix, quantidade

de *hosts* e *templates* ativos, além do número de itens e *triggers* configurados. Esses indicadores são importantes para avaliar a complexidade do ambiente monitorado e identificar possíveis pontos de atenção, como atualizações pendentes ou *hosts* sem monitoramento adequado.

O indicador de *Memory utilization* mostra o consumo de memória do servidor em torno de 21,27%, valor considerado saudável, garantindo que haja recursos disponíveis para execução das tarefas de monitoramento. O gráfico com o histórico, apresentado ao lado, reforça essa estabilidade, exibindo oscilações dentro de uma faixa de segurança.

A seção *Host availability* resume o status geral dos dispositivos: 1 disponível, 0 indisponível, 0 em estado misto e 7 com status desconhecido. Essa visão permite identificar de forma imediata problemas de conectividade ou falhas de comunicação entre o Zabbix e os equipamentos monitorados.

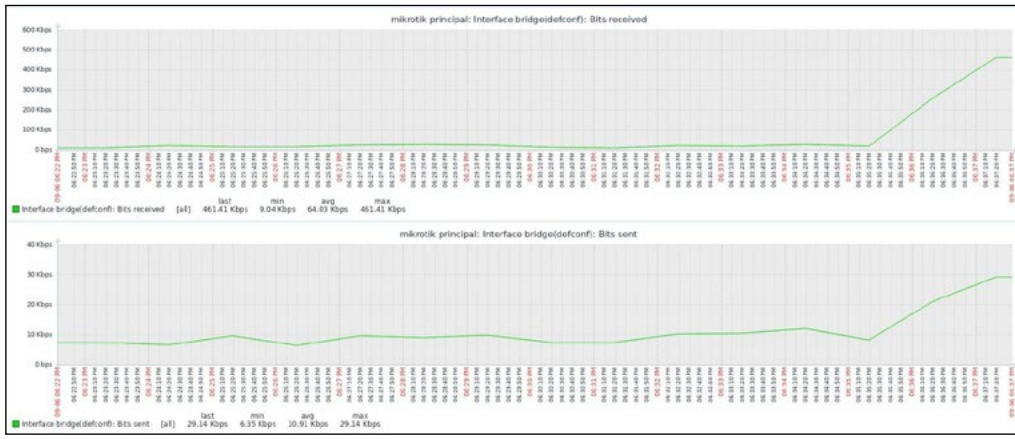
No quadro *Current problems*, são exibidos os eventos ativos. Destaca-se a indisponibilidade da central telefônica PABX, reportada pelo item ICMP Ping: *Unavailable*, e a falha na coleta de dados SNMP do Switch HPE OfficeConnect, ambos classificados com severidade alta. Essa categorização é essencial para priorizar a resolução dos incidentes mais críticos, garantindo a continuidade dos serviços de comunicação e rede.

Por fim, a seção *Problems by severity* classifica os eventos de acordo com sua gravidade, permitindo que o administrador da rede direcione esforços para os incidentes que representam maior risco operacional. Dessa forma, o *dashboard* global do Zabbix se consolida como uma ferramenta estratégica para o acompanhamento em tempo real da infraestrutura, oferecendo não apenas dados brutos, mas também indicadores visuais que facilitam a tomada de decisão e a rápida resposta a falhas.

Além desse monitoramento abrangente, foi possível implantar a supervisão de métricas importantes nos ativos da rede. Essas métricas fornecem conhecimentos valiosos sobre o desempenho e a saúde de cada dispositivo. Nesse sentido, foi implementado o monitoramento via protocolo SNMP para o roteador MikroTik RB3011UiAS, um ativo crítico para a infraestrutura de rede objeto deste estudo. Esta modalidade de monitoramento vai muito além da simples verificação de disponibilidade, assim, as principais métricas monitoradas incluíram:

- Taxa de transferência (*Throughput*): o monitoramento da taxa de transferência de dados fornece uma visão sobre a quantidade de dados que estão passando pelo ativo (Figura 14).

Figura 14 – Monitoramento do *throughput* do roteador MikroTik RB3011UiAS

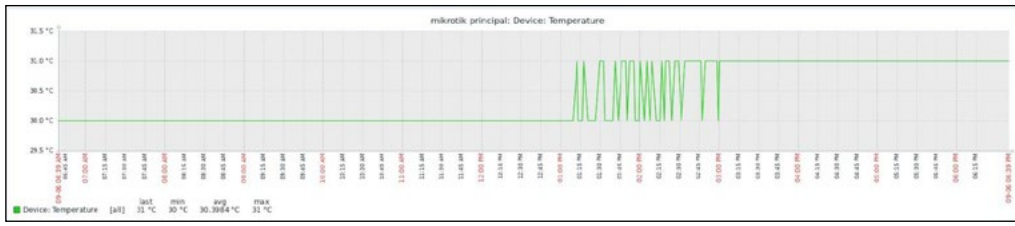


Fonte: Elaboração própria (2025).

O tráfego assimétrico observado, com aproximadamente 462 Kilobits por segundo recebidos e 29 Kilobits por segundo enviados é um indicador típico de padrão de taxa de download e upload. Monitorar essa métrica é crucial para identificar gargalos e validar a aderência aos contratos com provedores de serviços de internet, detectar anomalias e tráfego incomum como ataques de DDoS ou aplicações consumindo recursos de forma não autorizada e planejar a capacidade futura da rede com base em tendências históricas.

- Temperatura: o monitoramento da temperatura é essencial para prevenir o superaquecimento, que é um dos principais fatores capazes de prejudicar o desempenho e a vida útil dos ativos de rede (Figura 15).

Figura 15 – Monitoramento da temperatura do roteador MikroTik RB3011UiAS



Fonte: Elaboração própria (2025).

A métrica de Temperatura, com uma média de aproximadamente 30,5 °C no exemplo, é um indicador essencial da integridade física do equipamento, pois roteadores operando em temperaturas superiores às especificadas

pelo fabricante apresentam redução drástica de vida útil e podem sofrer reinicializações inesperadas.

Além disso, o monitoramento contínuo dessa variável permite não apenas a detecção precoce de condições de superaquecimento, mas também a emissão de alertas preventivos. Adicionalmente, possibilita avaliar a eficácia dos sistemas de ventilação e refrigeração do *data center* ou do *rack* e assegurar a estabilidade operacional do dispositivo, evitando degradações de desempenho decorrentes da ativação de mecanismos de proteção térmica.

- Capacidade de Armazenamento: o monitoramento do espaço total e utilizado no armazenamento interno é fundamental para a integridade do sistema. O MikroTik utiliza sua memória *flash* (*NAND*) para armazenar o sistema operacional (*RouterOS*), configurações, logs e pacotes adicionais (Figura 16).

Figura 16 – Monitoramento da memória de armazenamento do roteador MikroTik RB3011UiAS

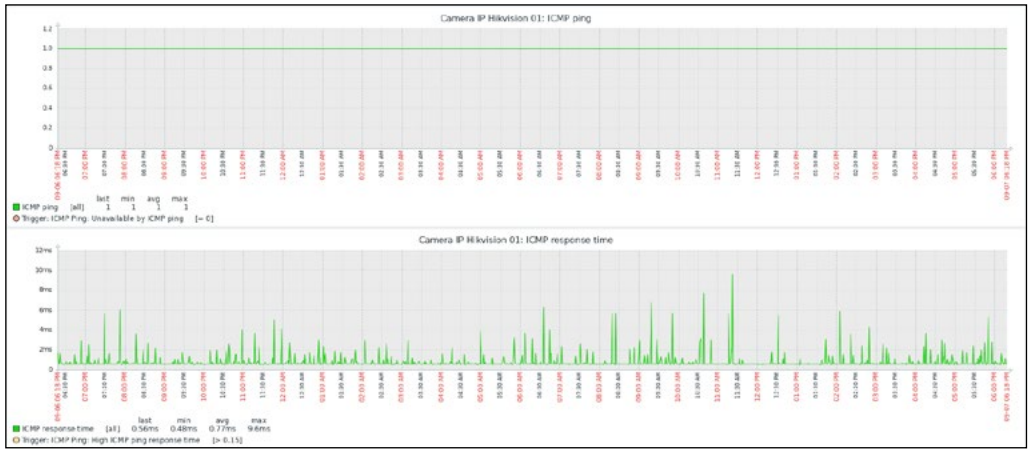
Fonte: Elaboração própria (2025).

A linha constante do gráfico de *Total space* evidencia a capacidade fixa do hardware, enquanto a métrica de *Used space* reflete o consumo dinâmico. O esgotamento desse espaço pode impedir atualizações críticas do *RouterOS*, deixando o dispositivo vulnerável, como também interromper a gravação de *logs* ou corromper o sistema de arquivos, exigindo intervenção manual para recuperação.

Finalmente, foi implementado o monitoramento para os demais ativos da rede. Diferentemente do roteador MikroTik RB3011UiAS, para o qual utilizou-se o protocolo SNMP, os switches, *access point*, câmeras IP, DVR, central telefônica PABX e telefones IP foram monitorados via ICMP.

Essa modalidade de monitoramento garante uma visão unificada da disponibilidade e da latência dos ativos, permitindo identificar rapidamente falhas de conectividade ou degradação de desempenho da rede. Como exemplo, a Figura 17 ilustra o monitoramento da câmera IP realizado por ICMP *Ping*, onde são evidenciados dois aspectos principais: a disponibilidade do dispositivo e a latência.

Figura 17 – Monitoramento da disponibilidade e latência câmera IP realizado por ICMP *Ping*



Fonte: Elaboração própria (2025).

Esse acompanhamento é fundamental para equipamentos de videomonitoramento, uma vez que a estabilidade da comunicação impacta diretamente na transmissão das imagens em tempo real. Picos de latência ou perda de pacotes podem resultar em travamentos, quedas na qualidade do vídeo ou até indisponibilidade temporária do dispositivo. Assim, o gráfico fornece ao administrador da rede uma ferramenta eficaz para diagnosticar e mitigar problemas relacionados ao desempenho e à confiabilidade da câmera dentro da infraestrutura monitorada.

Igualmente importante é o monitoramento dos switches e do *access point*, pois ambos atuam como concentradores do tráfego da rede, essenciais para a manutenção da conectividade dos usuários. A indisponibilidade ou instabilidade desses equipamentos pode comprometer toda a comunicação interna e o acesso aos serviços essenciais. Portanto, o acompanhamento contínuo desses dispositivos garante maior confiabilidade da infraestrutura, possibilitando uma resposta proativa a incidentes e contribuindo para a disponibilidade dos serviços.

5 CONSIDERAÇÕES FINAIS

Este artigo explorou a utilização da ferramenta, por meio de uma abordagem prática que envolveu a instalação, configuração e personalização, aplicada a um cenário real para o monitoramento de ativos de rede, visando melhorar a gestão, a segurança e a disponibilidade dos recursos de Tecnologia da Informação e Comunicação (TIC).

Inicialmente, foi realizada uma revisão bibliográfica, essencial para a consolidação dos conceitos teóricos relacionados ao gerenciamento de redes, protocolos de comunicação e ferramentas de monitoramento. Essa etapa mostrou-se indispensável para embasar a aplicação prática, permitindo uma compreensão aprofundada dos aspectos técnicos envolvidos.

Já o levantamento *in loco* dos ativos de rede presentes no laboratório possibilitou a identificação e catalogação de equipamentos, incluindo informações como fabricante, modelo e endereço IP. Esses dados foram cruciais para a adequada parametrização do sistema de monitoramento, assegurando a compatibilidade com os recursos oferecidos pelo Zabbix.

Finalmente, a implantação do ambiente de monitoramento envolveu a instalação do servidor Zabbix, a configuração de parâmetros específicos, bem como a utilização de *templates* nativos e personalizados. Essa etapa foi fundamental para adequar o sistema às necessidades da infraestrutura em análise, permitindo uma supervisão precisa e contínua do desempenho dos ativos.

A coleta de dados por meio dos protocolos ICMP e SNMP proporcionou uma visão abrangente da saúde da rede. Enquanto o ICMP permitiu verificar a disponibilidade dos dispositivos, o SNMP possibilitou a análise de métricas detalhadas como tráfego, uso de CPU e memória.

Durante a implementação, foram identificados desafios técnicos, como a configuração inicial dos dispositivos para responderem a requisições SNMP e a localização de identificadores OID adequados às métricas desejadas. Tais obstáculos foram superados com base em estudo dos protocolos e na exploração dos recursos nativos da ferramenta, como os *templates* predefinidos e as opções de monitoramento customizado.

Os resultados obtidos evidenciam que o Zabbix é uma solução eficaz, robusta e escalável para o monitoramento de ativos de rede. A ferramenta demonstrou ser capaz de fornecer informações em tempo real, emitir alertas automáticos em caso de anomalias, e, consequentemente, contribuir para o aumento da disponibilidade dos serviços e para a melhoria da segurança da infraestrutura de rede.

Conclui-se, portanto, que o Zabbix constitui uma ferramenta de fácil instalação e configuração inicial, especialmente devido à disponibilidade de *templates* prontos. O sistema mostrou-se altamente eficaz para o monitoramento

proativo de serviços, contribuindo significativamente para a redução do tempo de indisponibilidade percebido pelo usuário final.

Assim, a adoção de soluções de monitoramento baseadas em software livre como o Zabbix se apresenta como uma estratégia viável e recomendável no contexto da administração de redes de computadores, possibilitando a manutenção preditiva, com base em dados históricos e análise proativa, que representam um avanço significativo na gestão de redes.

Adicionalmente, o conhecimento adquirido durante a execução desta pesquisa fornece subsídios técnicos relevantes para futuras expansões do sistema de monitoramento, bem como para sua aplicação em ambientes de produção mais complexos.

REFERÊNCIAS

AGUIAR, Ítalo Fernandes. P**roposta de utilização da ferramenta Zabbix no gerenciamento de redes: um estudo de caso no ambiente da FAB segundo boas práticas de governança de TI. 2017.** 59 f. Monografia (Pós-Graduação em Gerência de Redes de Computadores e Tecnologia Internet) – Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2017. Disponível em: http://pantheon.ufrj.br/handle/11422/3300. Acesso em: 14 jul. 2025.

ALVES, Kaléu de Paula Soares. **Monitoramento de redes com Zabbix. 2021.** 42 f. Monografia (Graduação em Tecnologia em Redes de Computadores) – Faculdade de Tecnologia de Indaiatuba, Indaiatuba, 2021. Disponível em: https://ric.cps.sp.gov.br/handle/123456789/19027. Acesso em: 12 jul. 2025.

BARROS, Francisco. **Advanced Oracle monitoring agent for Zabbix. 2022.** 69 f. Dissertação (Mestrado Integrado em Engenharia Eletrotécnica e de Computadores) – Faculdade de Engenharia da Universidade do Porto, Porto, 2022. Disponível em: https://repositorio-aberto.up.pt/bitstream/10216/145449/2/592026.pdf. Acesso em: 30 jul. 2025.

BASSO, Douglas Eduardo. **Administração de redes de computadores.** Curitiba: Contentus, 2020.

DE OLIVEIRA, F.B.; PIRES, L.A.S.; GARCIA, J.P.C.S.; CAMÕES, R.J.S.; ALBUQUERQUE, R.O.; ALVES, J.S.F.; DE MENDONÇA, F.L.L.; NZE, G.D.A. Network Asset Management Supported by Best Practices for Resources Management and Monitoring. **RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação**, Porto, v. 2023, n. E62, p. 333–346, 2023. Disponível em: https://www.risti.xyz/issues/ristie62.pdf. Acesso em: 24 jul. 2025.

DEVMEDIA. **SNMP: Simple Network Management Protocol - Revista Infra Magazine 7**. 29 jul. 2025. DevMedia. Disponível em: https://www.devmedia.com.br/snmp-simple-network-management-protocol-revista-infra-magazine-7/25683. Acesso em: 12 jul. 2025.

GERMAIN, Jack M. **The Rise of Open Source: Pandemic, Economy, Efficiency, Trust.** 17 mar. 2021. LinuxInsider. Disponível em: https://www.linuxinsider.com/story/the-rise-of-open-source-pandemic-economy-efficiency-trust-87057.html. Acesso em: 7 jul. 2025.

GIAMATTEI, L.; GUERRIERO, A.; PIETRANTUONO, R.; RUSSO, S.; MALAVOLTA, I.; ISLAM, T.; DÎNGA, M.; KOZIOLEK, A.; SINGH, S.; ARMBRUSTER, M.; GUTIERREZ-MARTINEZ, J.M.; CARO-ALVARO, S.; RODRIGUEZ, D.; WEBER, S.; HENSS, J.; VOGELIN, E. Fernandez; PANOJO, F. Simon. Monitoring tools for DevOps and microservices: A systematic grey literature review. **Journal of Systems and Software,** Nova Iorque, v. 208, p. 01–24, fev. 2024. Disponível em: https://linkinghub.elsevier.com/retrieve/pii/S0164121223003011. Acesso em: 6 jul. 2025.

GUO, Fangming; CHEN, Caijun; LI, Ke. Research on Zabbix Monitoring System for Large-scale Smart Campus Network from a Distributed Perspective. **Journal of Electrical Systems,** Paris, v. 20, n. 10s, p. 631–648, 10 jul. 2024. Disponível em: https://journal.esrgroups.org/jes/article/view/5153. Acesso em: 14 jul. 2025.

HENTGES, Ramon; SCHORR, Maria Claudete. Monitoramento de redes de computadores utilizando o protocolo SNMP. **Revista Destaques Acadêmicos,** Lajeado, v. 13, n. 4, p. 145–164, 25 mar. 2022. Disponível em: http://univates.br/revistas/index.php/destaques/article/view/3037. Acesso em: 8 jul. 2025.

HUGHES, Owen. **Open source is more important than ever, say developers. Here's what's driving adoption.** 17 fev. 2022. ZDNET. Disponível em: https://www.zdnet.com/article/open-source-is-more-important-than-ever-say-developers-heres-why/. Acesso em: 7 jul. 2025.

KARA, Mehmet; TUĞRUL, Gökhan. **Efficiency of Adding a New Template to Network Management System and Zabbix Application.** *In*: 2025 7TH INTERNATIONAL CONGRESS ON HUMAN-COMPUTER INTERACTION, OPTIMIZATION AND ROBOTIC APPLICATIONS (ICHORA), 23 maio 2025. 2025 7th International Congress on Human-Computer Interaction, Optimization and Robotic Applications (ICHORA) [...]. Ankara, Turkiye: IEEE, 23 maio 2025. p. 1–6. Disponível em: https://ieeexplore.ieee.org/document/11017256/. Acesso em: 6 jul. 2025.

MACEDO, Ricardo Tombesi; FRANCISCATTO, Roberto; CUNHA, Guilherme Bernardino da; BERTOLINI, Cristiano. **Rede de computadores.** 1. ed. Santa Maria: Uab/Nte/Ufsm, 2018. Disponível em: https://repositorio.ufsm.br/bitstream/handle/1/18351/Curso_Lic-Comp_Redes-Computadores.pdf?sequence=1&isAllowed=y. Acesso em: 26 jul. 2025.

NOCTION. **Protocolo SNMP e Suas Traps: Explicação e Tendências.** 2023. Noction. Disponível em: https://www.noction.com/blog-pt/protocolo-snmp. Acesso em: 14 jul. 2025.

SILVA, Adelzemir Dos Santos Souza; SANTOS, Maria José Oliveira Dos; OLIVEIRA, Renato Almeida De. Estudo de gerenciamento de redes com Zabbix Server. **Brazilian Journal of Technology**, Curitiba, v. 7, n. 4, p. 01–24, 2 out. 2024. Disponível em: https://ojs.brazilianjournals.com.br/ojs/index.php/BJT/article/view/73272. Acesso em: 6 jul. 2025.

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. 01–10, 11 abr. 2024. Disponível em: https://ojs.focopublicacoes.com.br/foco/article/view/4851. Acesso em: 6 jul. 2025.

VALENTE, Júlia Miranda. **Monitoramento de ativos em uma rede de computadores de automação com aplicação da ferramenta Zabbix. 2023.** 61 f. Monografia (Graduação em Engenharia de Controle e Automação) – Universidade Federal de Ouro Preto, Ouro Preto, 2023. Disponível em: http://www.monografias.ufop.br/handle/35400000/5896. Acesso em: 14 jul. 2025.

ZABBIX. **Sobre a Zabbix LLC.** 2025. **The Enterprise-Class Open Source Network Monitoring Solution.** Disponível em: https://www.zabbix.com/br/about. Acesso em: 14 jul. 2025.