ESCOLA DE SAÚDE E FORMAÇÃO COMPLEMENTAR

1° Ten Al QCO LUCAS DOS REIS **DIAS**

1° Ten Al QCO LUCAS PIANISSOLA **DOS SANTOS**

1° Ten Al QCO CARLOS JORGE **MACHADO** DA SILVA SANTOS

1° Ten Al QCO BRUNO MOURA DO NASCIMENTO

1° Ten Al QCO TYAGO CAMPOS **MARTINS**

ESTUDO DE CASO DE IMPLEMENTAÇÃO E CONFIGURAÇÃO DA FERRAMENTA ZABBIX COMO PLATAFORMA DE UM AMBIENTE COMPUTACIONAL EM UMA ORGANIZAÇÃO MILITAR DO EXÉRCITO BRASILEIRO

SALVADOR

2024

1° Ten Al QCO LUCAS DOS REIS **DIAS**
1° Ten Al QCO LUCAS PIANISSOLA **DOS SANTOS**
1° Ten Al QCO CARLOS JORGE **MACHADO** DA SILVA SANTOS
1° Ten Al QCO BRUNO MOURA DO NASCIMENTO
1° Ten Al QCO TYAGO CAMPOS **MARTINS**

ESTUDO DE CASO DE IMPLEMENTAÇÃO E CONFIGURAÇÃO DA FERRAMENTA ZABBIX COMO PLATAFORMA DE UM AMBIENTE COMPUTACIONAL EM UMA ORGANIZAÇÃO MILITAR DO EXÉRCITO BRASILEIRO

Trabalho de Conclusão de Curso apresentado à Escola de Saúde e Formação Complementar do Exército como requisito parcial para a obtenção do grau de especialização em Aplicações Complementares às Ciências Militares.

Orientador: TC QCO **Tarcísio** do Nascimento Araújo.

Coorientador: Cap QCO Alexandre **Pinheiro**

SALVADOR

2024

Estudo de caso de implementação e configuração da ferramenta Zabbix como plataforma de um ambiente computacional em uma organização militar do Exército Brasileiro**.** ***/*** Lucas dos Reis Dias... [et al.]. - Salvador, 2024.

40 f.: 27,9 cm.

Trabalho de Conclusão de Curso do Curso (especialização) – Escola de Saúde e Formação Complementar do Exército, Salvador, 2024.
Orientador: TC QCO Tarcísio do Nascimento Araújo.

1. Zabbix. 2. Monitoramento. 3. ITIL. I. Dias, Lucas dos Reis. II. Título.

CDD 003

Elaborado por Patrícia Conceição Silva – CRB5/1669

1° Ten Al QCO LUCAS DOS REIS **DIAS**
1° Ten Al QCO LUCAS PIANISSOLA **DOS SANTOS**
1° Ten Al QCO CARLOS JORGE **MACHADO** DA SILVA SANTOS
1° Ten Al QCO BRUNO MOURA DO NASCIMENTO
1° Ten Al QCO TYAGO CAMPOS **MARTINS**

ESTUDO DE CASO DE IMPLEMENTAÇÃO E CONFIGURAÇÃO DA FERRAMENTA ZABBIX COMO PLATAFORMA DE UM AMBIENTE COMPUTACIONAL EM UMA ORGANIZAÇÃO MILITAR DO EXÉRCITO BRASILEIRO

Trabalho de Conclusão de Curso apresentado à Escola de Saúde e Formação Complementar do Exército como requisito parcial para a obtenção do grau de especialização em Aplicações Complementares às Ciências Militares.

Aprovado em 29 / 10 / 2024.

COMISSÃO DE AVALIAÇÃO

Documento assinado digitalmente
gov.br
TARCISIO DO NASCIMENTO ARAUJO
Data: 29/10/2024 09:32:44-0300
Verifique em https://validar.iti.gov.br

TARCÍSIO DO NASCIMENTO ARAÚJO **– Ten Cel**
Escola de Saúde e Formação Complementar do Exército
Presidente

Documento assinado digitalmente
gov.br
TIAGO DE FARIA
Data: 29/10/2024 15:46:59-0300
Verifique em https://validar.iti.gov.br

TIAGO **DE FARIA– Maj**
Escola de Saúde e Formação Complementar do Exército
Membro

Documento assinado digitalmente
gov.br
ALEXANDRE PINHEIRO
Data: 29/10/2024 13:00:52-0300
Verifique em https://validar.iti.gov.br

ALEXANDRE **PINHEIRO – Cap**
Escola de Saúde e Formação Complementar do Exército
Membro

RESUMO

O trabalho de conclusão de curso (TCC) intitulado "Estudo de Caso de Implementação e Configuração da Ferramenta Zabbix como Plataforma de Monitoramento em uma Organização Militar do Exército Brasileiro" tem como objetivo explorar a aplicação da ITIL (Information Technology Infrastructure Library) em conjunto com a ferramenta Zabbix e softwares complementares, visando o monitoramento de ativos de rede na Escola de Saúde e Formação Complementar do Exército (ESFCEx). Este estudo busca implementar um cenário da infraestrutura da ESFCEx, adotando as melhores práticas da ITIL. A pesquisa foca no monitoramento dos recursos computacionais através do Zabbix, priorizando a gestão da disponibilidade e capacidade dos serviços, alinhando-se à implementação da ITIL no Sistema de Telemática do Exército (SisTEx).

A metodologia adotada consiste em um estudo de caso que analisa métricas de latência, largura de banda e índice de disponibilidade, além de realizar uma análise comparativa com outras ferramentas disponíveis no mercado. Espera-se que os resultados levem a uma melhoria significativa na detecção e resolução de problemas, aumento da eficiência operacional e maior conformidade com os padrões de gestão de serviços de TI estabelecidos pela ITIL. A expectativa é que este estudo demonstre a viabilidade e os benefícios da integração entre ITIL e Zabbix, apresentando um modelo replicável para outras organizações militares.

Palavras-chave: Zabbix; Monitoramento; ITIL.

ABSTRACT

The conclusion work entitled "Case Study on the Implementation and Configuration of the Zabbix Tool as a Monitoring Platform in a Military Organization of the Brazilian Army," explores the integration of ITIL (Information Technology Infrastructure Library) with the Zabbix monitoring tool and complementary software for network asset monitoring at the Army School of Health and Complementary Training (ESFCEx). The study aims to implement a framework for ESFCEx's infrastructure, leveraging ITIL best practices. It focuses on monitoring computational resources through Zabbix, emphasizing service availability and capacity management, in alignment with ITIL implementation within the Army's Telematics System (SisTEx). The methodology includes a case study analyzing latency, bandwidth, and availability metrics, complemented by a comparative analysis of other market tools. Expected results include significant improvements in problem detection and resolution, enhanced operational efficiency, and greater compliance with IT service management standards established by ITIL. Ultimately, this study aims to demonstrate the feasibility and benefits of integrating ITIL and Zabbix, providing a replicable model for other military organizations.

Keywords: Zabbix; Monitoring; ITIL.

LISTA DE FIGURAS

SUMÁRIO

1. INTRODUÇÃO

As tecnologias são desenvolvidas para atender as demandas dos setores intensivos em informação. Diante dessa perspectiva, gerenciar os serviços de Tecnologia da Informação (TI) para que estejam alinhados com os objetivos de uma organização é imprescindível. No entanto, os setores de informática muitas vezes lidam com um volume grande de dados e nem sempre conseguem lidar com eles para que se solucione da melhor maneira possível os desafios que surgem durante o ciclo de vida das empresas, exigindo assim um gerenciamento mais efetivo e inteligente dos serviços como um todo (Tigre, 2006).

Transversal a esse cenário está o contexto militar, onde surge a figura do Centro Integrado de Telemática do Exército (CITEx), baseado na Portaria nº 077-Cmt Ex (2019), organização subordinada ao Departamento de Ciência e Tecnologia (DCT) e que está atualmente estruturado em sete Centros de Telemática de Área (CTAs) e cinco Centros de Telemática (CTs). Esses centros apoiam as Organizações Militares (OMs) e juntos formam o Sistema de Telemática do Exército (SisTEx). Ademais, o SisTEx possui um Catálogo de Serviços de Tecnologia da Informação (CSTI) fundamentado nas diretrizes da ITIL. (Centro Integrado de Telemática do Exército, 2018).

O SisTEx oferece suporte a diversas capacidades e o CSTI especifica quais serviços estão disponíveis, o tempo necessário para atender cada demanda e outros procedimentos relevantes. Entre os serviços oferecidos, destacam-se: acesso à internet, gerenciamento de e-mail, consultoria técnica, suporte para captura de imagens, acesso à Virtual Private Network (VPN), hospedagem e disponibilidade de sistemas, hospedagem de páginas das OMs na internet, acesso à telefonia, proteção cibernética, entre outros (Centro Integrado de Telemática do Exército, 2018). Em cada OM do Exército há uma divisão ou seção de informática pertencente ao SisTEx que realiza algumas dessas atividades, sendo que na Escola de Saúde e Formação Complementar do Exército (ESFCEx) cumpre a Divisão de Tecnologia da Informação (DTI) a gerência de alguns dos serviços listados.

O contexto apresentado acima será abordado dentro da estrutura da ESFCEx por meio do serviço de acesso à internet que possibilita à OM acessar a rede mundial de computadores e a Rede EBNET, sendo que a última realiza a função de

intranet na instituição, oferecendo um acesso com maior segurança, disponibilidade e integridade aos dados trafegados do que um link de Internet convencional (Centro Integrado de Telemática do Exército, 2018). Além disso, será abordada o suporte a infraestrutura para hospedagem de sistemas, tais como o Ambiente Virtual de Aprendizagem (AVA), o qual corresponde a capacidade de hospedagem de sistemas regionais do SisTEx.

Para auxiliar essa demanda será realizado um estudo alinhado às diretrizes da ITIL, dentro dos critérios estabelecidos pelo SisTEx utilizando para isso o Zabbix, uma ferramenta de monitoramento de redes e serviços amplamente utilizada em ambientes corporativos de TI. Ela permite a coleta, análise e visualização de dados de desempenho e disponibilidade de diversos componentes de infraestrutura, como servidores, bancos de dados, dispositivos de rede, aplicativos, e serviços em nuvem. Sua capacidade de monitorar grandes volumes de dados em tempo real, aliada a um sistema robusto de notificações e alertas, o torna uma escolha estratégica para empresas que buscam garantir a continuidade e a eficiência de suas operações (Zabbix SIA, 2024a).

Dado a implementação do SisTEx no Exército usando o ITIL, este trabalho propõe explorar as melhores práticas adotadas na biblioteca alinhado com a utilização da ferramenta Zabbix, a fim de fornecer recomendações e soluções para otimizar a disponibilidade, segurança e qualidade dos serviços oferecidos pela ESFCEx.

1.1 PROBLEMA

A necessidade de uma ferramenta de monitoramento dos ativos de rede que esteja implementada em um modelo que correlacione os serviços prestados pelo SisTEx agrupado conforme a metodologia da ITIL em funcionamento no âmbito do Exército Brasileiro.

1.1.1 Antecedentes do Problema

Considerando ser um ambiente de formação militar e a importância dos serviços de hospedagem de sistemas e acesso à internet, presentes no catálogo de serviços do SisTEx, os problemas de indisponibilidade trazem uma série de consequências e complicações para as atividades-fim da instituição. (Aguiar, 2017). Torna-se necessário, portanto, considerar uma solução viável, adaptada e integrada para receber os alertas e atuar em tempo hábil na solução dos incidentes, tudo isso de maneira sistematicamente adaptada ao modelo de governança ITIL implementado no Âmbito do SisTEx.

1.1.2 Formulação do Problema

Dessa forma, essa seção busca detalhar a demanda do monitoramento conforme o Desenho e Operação dos Serviços dividindo-os em categorias baseadas nas classificações utilizadas pela biblioteca ITIL:

1.1.2.1 Gestão de Incidentes

Resposta a Emergências: A falta de alertas compromete a capacidade de resposta rápida a falhas críticas, afetando a continuidade dos serviços essenciais (Office of Government Commerce, 2007).

1.1.2.2 Gestão de Problemas

a) Análise de Causa Raiz: Sem dados sobre incidentes recorrentes, torna-se mais difícil identificar e resolver problemas subjacentes (Bon, 2012).
b) Prevenção de Problemas: A falta de informações impede a identificação de padrões que poderiam ser abordados preventivamente (Office of Government Commerce, 2007).

1.1.2.3 Gestão da Disponibilidade

Confiabilidade Reduzida: A ausência de alertas diminui a capacidade de manter a disponibilidade e a confiabilidade dos serviços (Bon, 2012).

1.2 OBJETIVOS

Propor um modelo de monitoramento dos serviços providos pelo SisTEx, de acordo com as bibliotecas da ITIL implantadas no Exército brasileiro, utilizando, para isso as ferramentas Zabbix e Grafana.

1.2.1 Objetivo Geral

Prover um modelo de monitoramento dos recursos computacionais fornecidos utilizando à ferramenta Zabbix em um ambiente que simula a infraestrutura da ESFCEx, baseado na implementação do ITIL no âmbito do SisTEx de modo a trazer eficiência e eficacia na prestação dos serviços propostos em seu catálogo de serviço.

1.2.2 Objetivo Específico

Com a finalidade de delimitar e alcançar o desfecho esperado para o objetivo geral, foram levantados objetivos específicos que conduziram à consecução do objetivo deste estudo, os quais são transcritos abaixo:

1. Implementar um modelo de monitoramento do serviço de internet que permita identificar incidentes e solucionar problemas que possam comprometer a disponibilidade do serviço.
2. Implementar um modelo de monitoramento do serviço de hospedagem de sistema que permita identificar incidentes e solucionar problemas que possam comprometer a disponibilidade do serviço.
3. Identificar as métricas que serão utilizadas como parâmetro para avaliar o desempenho dos serviços monitorados.

1.3 Questões de Estudo

a. O modelo de monitoramento proposto é adequado ao funcionamento de uma seção de informática de uma OM?
b. É possível integrar o Zabbix ao Grafana?
c. É possível identificar métricas adequadas ao desenho e operação do serviço conforme implantado SisTEx?

1.4 Metodologia

A pesquisa adotou a metodologia exploratória em conjunto com abordagens experimentais e revisão bibliográfica.

Um ambiente simulado foi criado para os testes, utilizando os softwares Zabbix e Grafana para emular os serviços a serem monitorados a fim de conduzir o experimento proposto.

O modelo implementado no ambiente de simulação foi elaborado conforme as métricas identificadas no decorrer da pesquisa em consonância com o desenho e operação de serviço da ITIL no âmbito do Exército Brasileiro.

E, no que diz respeito à simulação do ambiente, foi usada uma máquina virtual com o sistema operacional Linux, na qual foram instalados softwares já citados, buscando uma representação do ambiente do SisTEx em funcionamento no âmbito da ESFCEx.

A pesquisa bibliográfica fundamentou-se nos procedimentos relativos às temáticas relacionadas às ferramentas de monitoramento de ativos mais utilizadas no mercado, documentação no âmbito do SisTEx referente ao funcionamento do ITIL e ao catálogo de serviços.

A pesquisa seguiu uma abordagem qualitativa, concentrando-se na exploração e compreensão dos significados, percepções e benefícios decorrentes da implementação de um modelo que monitoramento dos serviços de gestão de incidentes, problemas e disponibilidade.

1.4.1 Objeto Formal de Estudo

O presente estudo tem como objeto a análise do modelo implementado na ferramenta de monitoramento Zabbix para a gestão de incidentes, disponibilidade e problemas conforme implementação do ITIL no âmbito do SisTEx e em conformidade com seu catálogo de serviço. Utilizando-se de uma simulação do ambiente de TI da ESFCEx.

1.4.2 Delineamento da Pesquisa

Este estudo segue um delineamento de pesquisa aplicada com um enfoque exploratório e descritivo. O objetivo principal é avaliar a eficácia da ferramenta Zabbix na gestão e monitoramento de ativos de rede na ESFCEx, em consonância com as práticas recomendadas pela ITIL.

O delineamento da pesquisa foi estruturado em três fases principais:

Fase de Preparação e Planejamento:

a) Revisão da literatura sobre monitoramento de redes, Zabbix, e ITIL para fundamentar a escolha das ferramentas e práticas adotadas.
b) Definição dos objetivos específicos da implementação e identificação dos ativos de rede e serviços críticos a serem monitorados.

Fase de Implementação:

a) Configuração inicial do Zabbix e integração com outros sistemas relevantes, como o Grafana para visualização de dados.
b) Implementação do monitoramento de ativos de rede específicos, seguindo as diretrizes e *templates* sugeridos pelo Zabbix, com foco na detecção de falhas e na otimização da disponibilidade dos serviços.
c) Coleta de dados em tempo real, incluindo métricas de desempenho, incidentes detectados e tempos de resposta.

Fase de Análise e Discussão:

a) Análise dos dados coletados à luz dos conceitos e práticas da ITIL, com especial atenção à gestão de incidentes, problemas, disponibilidade e capacidade.
b) Discussão dos resultados obtidos, destacando as melhorias observadas na infraestrutura da ESFCEx e os desafios encontrados durante a implementação.

Este delineamento permite uma abordagem sistemática e organizada do estudo, garantindo que os objetivos do trabalho sejam alcançados de maneira clara e objetiva.

1.4.3 Procedimentos para Revisão da Literatura

Foram selecionadas bases de dados eletrônicas pertinentes à área de estudo, abrangendo bibliotecas digitais, repositórios de teses e dissertações, periódicos científicos, entre outras fontes relevantes. Além disso, fontes alternativas de busca também foram levadas em consideração, como livros especializados e artigos apresentados em conferências de relevância. No processo de busca, foram identificadas palavras-chave e termos relacionados ao tópico de pesquisa, incluindo Zabbix, monitoramento, Grafana, ITIL e métricas de avaliação de desempenho.

1.4.4 Procedimentos Metodológicos

A revisão da literatura deste trabalho teve como foco principal a compreensão detalhada do Zabbix, do conceito de monitoramento de sistemas de TI, do Grafana, e de outras ferramentas relevantes no mercado. Para alcançar esse objetivo, foram seguidas as etapas descritas a seguir.

Primeiramente, foi realizada uma pesquisa bibliográfica em livros, artigos científicos, documentações técnicas relacionadas ao monitoramento de redes e sistemas de TI.

Em seguida, a revisão abordou o conceito de monitoramento de TI em um contexto mais amplo. Foram estudados os principais tópicos relacionados ao monitoramento, como a importância da observação contínua de sistemas para a prevenção de falhas, a coleta e análise de dados em tempo real, e a implementação de boas práticas de governança de TI, conforme prescrito pela ITIL.

O Grafana também foi investigado como uma ferramenta complementar ao Zabbix, com foco em suas capacidades de visualização de dados. A revisão literária explorou como o Grafana pode ser integrado ao Zabbix para criar dashboards detalhados que permitem a análise de métricas em tempo real.

Por fim, a revisão comparou o Zabbix com outras ferramentas de monitoramento disponíveis no mercado, como Nagios, Icinga, Prometheus e PRTG. Essa comparação incluiu a análise das características, vantagens e desvantagens de cada ferramenta, com o intuito de justificar a escolha do Zabbix como a solução mais adequada para o monitoramento.

1.4.5 Instrumentos

O processo de construção do conhecimento teve seu início com uma análise minuciosa dos documentos e tutoriais encontrados na internet, os quais abordam o tópico em questão. Além disso, como instrumento para a simulação do modelo proposto, foi utilizada a ferramenta Zabbix, e, para a visualização desses dados, optou-se pela integração com os gráficos do Grafana, que oferece uma interface mais amigável e rica em funcionalidades visuais. Além disso, para a simulação dos cenários, foram utilizadas máquinas virtuais, permitindo maior flexibilidade e controle sobre os testes.

1.4.6 Análise da simulação

Os dados obtidos através das simulações realizadas foram organizados e categorizados conforme a relevância. Foram estabelecidos métricas para facilitar a análise e interpretação dos dados.

Os resultados e conclusões foram apresentados de forma clara e coerente, utilizando trechos de citações e outras representações visuais, conforme apropriado.

A análise da simulação foi realizada com base no modelo proposto, com ênfase no gerenciamento de incidente e disponibilidade e na gestão de problemas. Para comparar os parâmetros ideais, estabelecidos na pesquisa, com os resultados obtidos, foi realizada uma pesquisa eletrônica em sites de instituições acadêmicas, artigos publicados em periódicos especializados e livros renomados da área de Tecnologia da Informação.

1.5 JUSTIFICATIVA

Tendo em vista os aspectos apresentados, o uso dos princípios do ITIL nesse trabalho se justifica pelo fato de estar presente no catálogo de serviço do SisTEx, sendo um conjunto de melhores práticas, desenvolvido e estudado e muito utilizado nos ambientes corporativos.

O monitoramento de serviços de TI, conforme descrito na ITIL, envolve a coleta contínua de dados sobre o desempenho e a disponibilidade dos sistemas, permitindo uma gestão proativa e a rápida resolução de problemas. No contexto educacional, monitorar a infraestrutura dos serviços de hospedagem e a situação dos links de internet são cruciais para garantir que os alunos e professores tenham acesso contínuo e confiável aos recursos necessários para o processo de ensino e aprendizagem.

2. REVISÃO DE LITERATURA

2.1 MONITORAMENTO

A importância das redes de computadores para o funcionamento das empresas vem crescendo significativamente. Atualmente, elas são consideradas uma infraestrutura essencial e de missão crítica, ou seja, a interrupção dessas redes pode causar impactos severos nas operações (Janssen, 2020). No entanto, manter a rede totalmente operacional não é suficiente se os serviços oferecidos por ela, que são o foco principal dos clientes, não estiverem funcionando corretamente.

Com base nesse conceito, é fundamental definir com precisão quais serviços devem ser monitorados e por que esse monitoramento é necessário. A identificação dos componentes críticos da rede não deve ser uma responsabilidade exclusiva da

equipe de tecnologia da informação (TI). Pelo contrário, é essencial que haja uma colaboração entre os diversos setores da empresa (Janssen, 2020). Somente com a participação dos gestores de todas as áreas será possível realizar um levantamento completo dos ativos e serviços que precisam ser monitorados. Esse processo colaborativo permite definir o que realmente deve ser acompanhado para garantir que a rede e seus serviços estejam sempre disponíveis e funcionando conforme o esperado.

Além disso, é importante ressaltar que o monitoramento adequado não apenas evita falhas, mas também otimiza o desempenho da rede e garante a segurança dos dados. Soluções automatizadas podem alertar as equipes de TI sobre possíveis problemas antes que eles afetem os serviços, permitindo uma resposta proativa e minimizando os riscos operacionais. Essa abordagem integrada de monitoramento proporciona uma visão completa da infraestrutura, melhorando a tomada de decisões e permitindo que as empresas ofereçam serviços mais confiáveis e eficientes.

2.2 DISPONIBILIDADE

A gestão da disponibilidade na ITIL busca assegurar que os serviços e componentes possam coletar dados para medir a disponibilidade. Essas medições incluem a satisfação do usuário, o tempo perdido devido à indisponibilidade do serviço, o número de transações perdidas e o impacto na produtividade. O objetivo desse gerenciamento é garantir o cumprimento dos SLAs acordados com os usuários (Axelos, 2019). Ressalta-se que o CSTI do SisTEx também se concentra nesse aspecto em todas as suas capacidades oferecidas (Centro Integrado de Telemática do Exército, 2018).

Nesse contexto, a notificação da indisponibilidade de um serviço pode ocorrer de duas maneiras: pelo usuário, que a reporta quando está insatisfeito, ou por meio de um sistema de monitoramento (Duman; Eli̇iyi̇, 2021). Neste último caso, a abordagem se revela mais eficaz, pois permite uma reação mais rápida e não compromete a primeira medição apresentada no gerenciamento da disponibilidade.

Essa proatividade no monitoramento é fundamental para garantir a continuidade dos serviços e a satisfação do usuário.

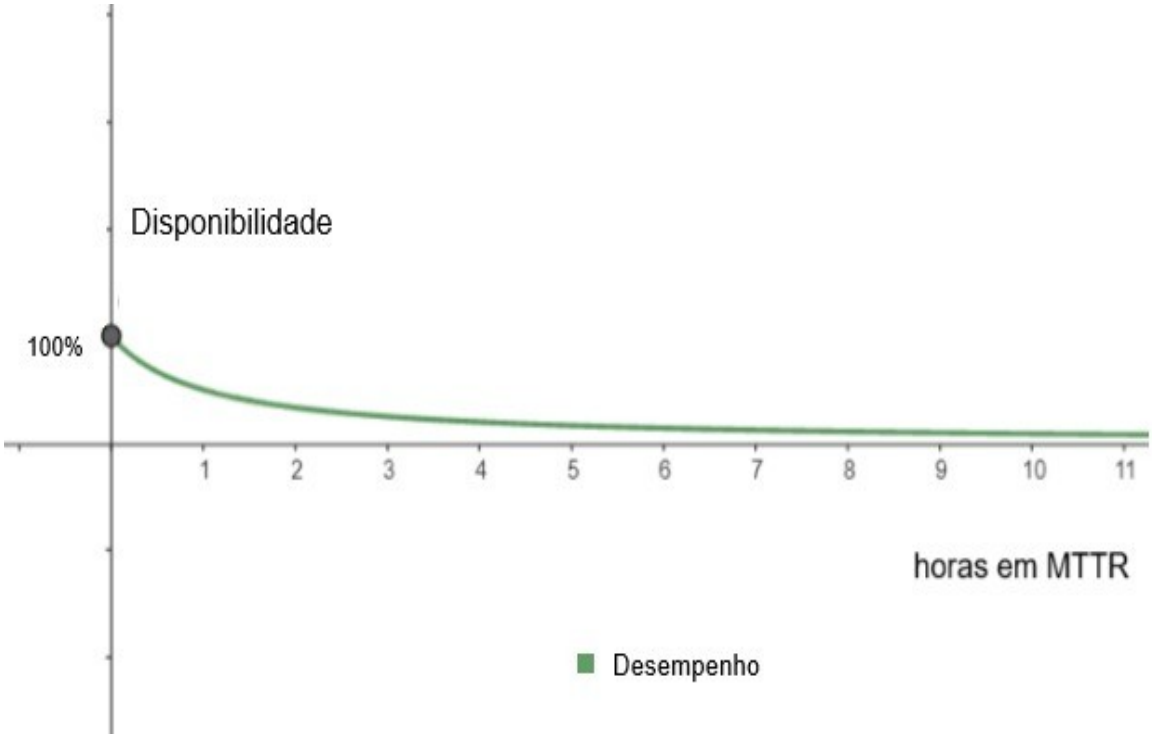
Complementando essa perspectiva, Bon (2012) enfatiza que é essencial manter a confiança dos clientes e responder de maneira eficaz a incidentes. Para isso, usa as métricas de tempo médio entre falhas (MTBF) e de tempo médio de reparo (MTTR) que permitem identificar áreas de melhoria e medições da qualidade do serviço acordado. Nesse sentido, o CSTI estabelece um MTTR para a capacidade de acesso à Internet em casos de indisponibilidade ou lentidão (Centro Integrado de Telemática do Exército, 2018).

Essas métricas apresentam diferentes graus de importância. Serviços mais antigos eram frequentemente projetados com um MTBF elevado, resultando em raras falhas. No entanto, recentemente, houve uma mudança de enfoque para otimizar o design dos serviços, visando reduzir o MTTR, permitindo uma recuperação mais ágil (Axelos, 2019). Duman e Eli̇iyi̇ (2021) demonstraram a importância dessa métrica na gestão da disponibilidade ao analisarem sua fórmula, conforme descrito na biblioteca da ITIL. Essa fórmula calcula a razão entre o MTBF e a soma do MTBF com o MTTR (Bon, 2012, Duman; Eli̇iyi̇, 2021). Com o uso de limites é possível perceber a diferença de importância das duas métricas, tomando como variável o MTTR tendendo ao infinito pela direita e tomando um valor constante para o MTBF, conforme Equação 1.

$$\lim_{MTTR \to \infty^+} \frac{MTBF}{MTBF + MTTR} \tag{1}$$

A Figura 1 apresenta graficamente essa análise, onde o eixo das ordenadas indica um valor máximo de uma unidade, correspondente a 100% de disponibilidade. Para atingir essa porcentagem, o tempo para o MTTR deve ser nulo. Por outro lado, o eixo das abscissas ilustra que, à medida que o MTTR tende ao infinito, a disponibilidade do sistema diminui, aproximando-se de zero. Essa representação gráfica evidencia a importância do MTTR, corroborando as discussões anteriores sobre a necessidade de otimização para garantir um serviço de qualidade.

Figura 1: Gráfico da Disponibilidade



Fonte: O autor.

Diante disso, para garantir um bom MTTR, o tempo é um fator crucial; quanto mais rápido um incidente for resolvido, melhor será a disponibilidade do serviço. Para isso, é fundamental que o administrador seja notificado do incidente ocorrido o mais breve possível.

2.3 CAPACIDADE

Após discutir a importância da gestão da disponibilidade e as métricas relacionadas ao desempenho dos serviços de TI, é fundamental abordar o gerenciamento de capacidade, conforme definido pela ITIL. Este gerenciamento visa assegurar que a capacidade dos serviços e da infraestrutura de TI atenda aos requisitos acordados e promova um desempenho eficaz (Cabinet Office, 2011). Esse desempenho é medido pela quantidade máxima que um item de configuração ou

serviço pode oferecer (Axelos, 2019). Além disso, o gerenciamento de capacidade busca atender tanto às necessidades atuais quanto às futuras de desempenho e capacidade do negócio (Cabinet Office, 2011).

Para facilitar essa abordagem, Bon (2012) e Cabinet Office (2011) identificam três subprocessos principais dentro do gerenciamento de capacidade: capacidade de negócios, capacidade de serviços e capacidade de componentes. A capacidade de negócios, em particular, foca na identificação de tendências e na previsão das necessidades futuras, operando em um nível estratégico. Por meio dessas atividades, as organizações podem antecipar picos de demanda e ajustar a infraestrutura de TI conforme necessário.

No que diz respeito à capacidade de serviços, este subprocesso se concentra na gestão de serviços de ponta a ponta, posicionando-se em um nível tático. Nessa capacidade, a atenção se volta para parâmetros essenciais, como a taxa de transferência de transações e o tempo de resposta. Por outro lado, a capacidade de componentes é responsável pelo monitoramento dos elementos individuais da infraestrutura de serviço, incluindo discos, processadores e conexões de rede (Cabinet Office, 2011). Neste contexto, a DTI da escola se dedica a focar seus serviços na capacidade de serviços, permitindo o monitoramento do tempo de resposta do link de internet.

Ao aprofundar-se no tempo de resposta, é crucial entender como ele influencia não apenas a eficiência operacional, mas também a satisfação do usuário (Ferreira, 2023). Essa satisfação, por sua vez, impacta diretamente o gerenciamento da disponibilidade, conforme discutido na seção anterior, destacando a interconexão entre esses elementos no contexto da gestão de TI.

Devido à relevância dessa métrica, é importante entender que o tempo de resposta é composto pela soma do tempo de comunicação entre dois serviços e do tempo de processamento em cada sistema. O tempo de comunicação refere-se ao intervalo entre o envio de uma mensagem pelo emissor e o seu recebimento pelo destinatário, enquanto o tempo de processamento é o período que cada parte leva para compreender os dados recebidos (Cotta, 2020). A interação entre o tempo de comunicação e o tempo de processamento determina a rapidez com que as informações são trocadas, impactando diretamente a percepção do serviço.

Além disso, Grigorik (2013) indica que um tempo de resposta superior a 300 milissegundos pode comprometer a experiência em plataformas digitais interativas.

Portanto, é crucial manter esse tempo abaixo de 250 milissegundos para garantir o engajamento do usuário, refletindo a importância de monitorar e otimizar constantemente essas métricas para promover uma experiência satisfatória.

2.4 Métricas

Nesta seção, serão apresentadas as métricas utilizadas para a avaliação do desempenho dos equipamentos que compõem a infraestrutura relacionada aos serviços monitorados citados anteriormente, a saber: disponibilidade e capacidade.

As métricas estipuladas abrangem não apenas os ativos de rede, como switches e roteadores, mas também servidores físicos e máquinas virtuais, garantindo uma análise completa de todo o ambiente.

As métricas definidas incluem latência, largura de banda e índice de disponibilidade, sendo reconhecidos como essenciais para mensurar o desempenho do serviço prestado. Vale ressaltar que essas métricas podem ser ajustadas conforme a especificidade de cada cenário. A seguir, serão apresentadas as métricas utilizadas.

2.4.1. Latência

Definiu-se como parâmetro que valores de latência abaixo de 100 ms seriam considerados adequados, conforme padrão adotado pela maioria das empresas (Kernitskyi, 2024). Esse critério estabelece uma referência clara sobre a qualidade do serviço em termos de tempo de resposta da rede.

2.4.2. Largura de banda

No ambiente simulado, considerou-se um link contratado de 1000 Mbps, estabelecendo-se que uma utilização superior a 70% da capacidade total (ou 700 Mbps) seria considerada alta, e uma utilização inferior a 50% (ou 500 Mbps), caracterizaria subutilização, demandando atenção para possível ociosidade. Os valores estabelecidos para este critério são aqueles comumente utilizados pelas OMs do SisTEx.

2.4.3. Índice de disponibilidade

Para o cálculo da disponibilidade, foi empregada a seguinte fórmula:

$$Disponibilidade = \frac{Tempo\ Disponível}{Tempo\ Máximo}$$

Os termos que constituem a fórmula de disponibilidade são descritos detalhadamente a seguir:

- **Disponibilidade** - A disponibilidade representa o percentual de tempo em que um serviço ou recurso está operando corretamente dentro de um intervalo de tempo específico. O resultado é expresso como uma fração ou porcentagem, e valores mais próximos de 1 (ou 100%) indicam maior disponibilidade.
- **Tempo disponível** - Este termo refere-se ao período em que o sistema ou serviço esteve efetivamente funcionando e acessível para os usuários. Ou seja, é o tempo durante o qual o sistema estava operacional e não sofreu interrupções. Esse tempo pode ser padronizado em horas, minutos, ou segundos, dependendo do intervalo estabelecido no acordo de nível de serviço e conforme dado obtido pela ferramenta.
- **Tempo total possível** - O tempo total possível é o período completo de observação durante o qual o sistema foi monitorado. Representa o tempo máximo em que o sistema poderia estar funcionando sem interrupções. Normalmente, esse valor é o mesmo para todos os cálculos de disponibilidade dentro de um determinado intervalo.

2.4.3.1 Exemplo de Aplicação

Suponha que estamos avaliando a disponibilidade de um sistema ao longo de 24 horas. Se o sistema ficou disponível e operacional durante 23 horas, o cálculo seria:

$$Disponibilidade = \frac{23h}{24h} = 0{,}9583\ ou\ 95{,}83\%$$

Esse índice permite avaliar a eficiência do sistema, com foco em maximizar o tempo disponível e aprimorar a continuidade dos serviços.

2.4.3.1 Análise Comparativa das Métricas

Ao analisar as métricas selecionadas, é possível correlacioná-las com o desenho e operação do serviço, obtendo-se o quadro abaixo (Quadro 1).

Quadro 1 – Análise comparativa de métricas

Métrica/ITIL	Disponibilidade	Capacidade	Problema
Latência	Não atende	Atende	Atende
Largura de banda	Não atende	Atende	Atende parcialmente
Índice de disponibilidade	Atende	Não atende	Não atende

Fonte: O autor.

Ao analisar as métricas apresentadas no quadro 1, observa-se que a métrica de Índice de Disponibilidade é mais adequada à gestão da disponibilidade, e a Largura de Banda está relacionada à gestão de capacidade, assim como a Latência

atende a gestão de problema. Deste modo, o modelo de monitoramento proposto buscou implementar os critérios acima estabelecidos.

2.5 FERRAMENTAS DO MERCADO

A seguir, serão apresentadas algumas ferramentas do mercado que podem realizar tanto o monitoramento da disponibilidade quanto da capacidade dos serviços gerenciados pela DTI da ESFCEx. Além disso, será realizada uma análise comparativa entre essas ferramentas, permitindo uma avaliação mais aprofundada de suas funcionalidades. Também será destacado o Grafana, um sistema que oferece painéis visuais que facilitam a tomada de decisões ao representar graficamente os dados monitorados.

2.5.1 Zabbix

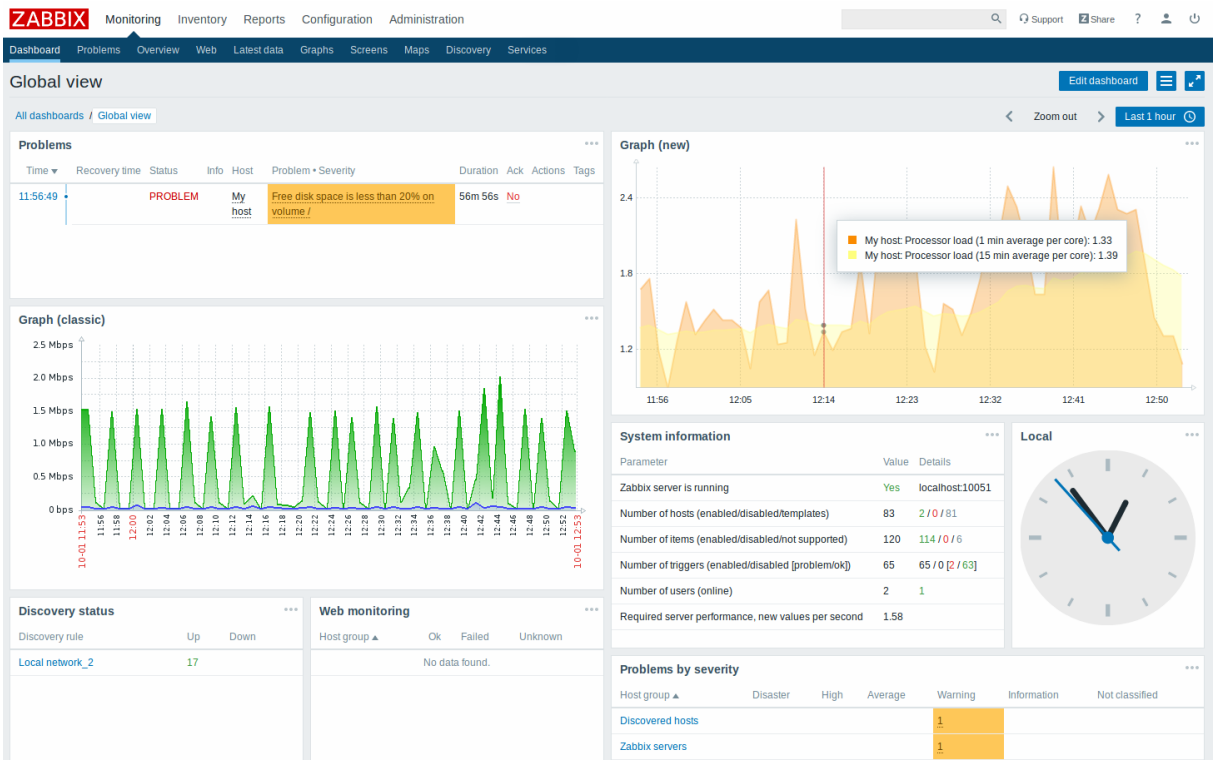
O Zabbix é uma plataforma *open-source*[1] robusta e amplamente utilizada para o monitoramento de infraestrutura de TI, redes, servidores, aplicações e serviços. Ele permite a coleta de dados em tempo real, a criação de alertas e a visualização de métricas através de *dashboards*[2] personalizados (Janssen, 2020).

2.5.1.1 Arquitetura

Entre os principais componentes do Zabbix, destacam-se o Zabbix Server, que é o núcleo central responsável pelo processamento de dados de monitoramento, o Zabbix Agent, instalado nos hosts monitorados para coletar informações detalhadas, e o Zabbix Frontend, uma interface web que oferece aos usuários acesso às configurações, dashboards e relatórios. Essa arquitetura

modular permite que o Zabbix se integre a uma vasta gama de sistemas e plataformas, proporcionando uma gestão centralizada e eficaz dos recursos de TI (Janssen, 2020). Um exemplo de dashboard do Zabbix é apresentado na Figura 2.

Figura 2: Dashboard do Zabbix

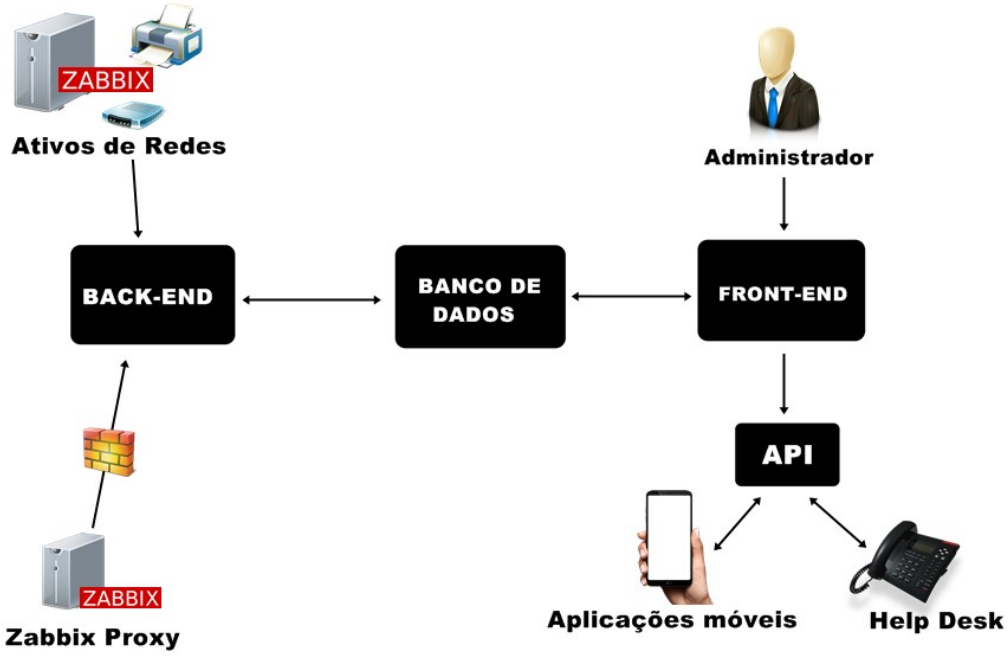


Fonte: Zabbix SIA, 2024a

A arquitetura do Zabbix é composta por três elementos principais, conforme ilustrado na Figura 3. A coleta de dados dos ativos de rede é realizada pelo *backend*, que opera nos bastidores do sistema, processando e gerenciando as informações sem interação direta com o usuário. Esses dados são armazenados na camada de banco de dados, responsável por organizar e disponibilizar as informações para o *frontend*, que é a interface interativa acessada pelo usuário final. A interface web, gerenciada pelo *frontend*, permite que os administradores acessem e monitorem os dados de forma prática, além de oferecer suporte a integração via API do Zabbix (Zabbix SIA, 2024a).

[1] Open source é um termo em inglês que significa "código aberto", referindo-se a software desenvolvido de forma descentralizada e colaborativa, com revisão e produção pela comunidade, sendo geralmente mais barato, flexível e duradouro do que opções proprietárias (Red Hat, Inc., 2024).
[2] Dashboards são painéis que permitem visualizar dados graficamente, proporcionando uma representação clara e concisa de informações importantes.

Figura 3: Arquitetura do Zabbix



Fonte: Bernardo, 2024

2.5.1.2 Funcionalidades

O Zabbix oferece diversas funcionalidades que garantem o monitoramento eficiente de infraestruturas de TI, permitindo coleta de dados, alertas e visualizações configuráveis (Zabbix SIA, 2024a).

2.5.1.2.1 Coleta de Dados

A coleta de dados no Zabbix oferece uma gama de opções para verificar a disponibilidade e o desempenho dos dispositivos monitorados. A solução é compatível com diversos protocolos e tecnologias, como SNMP (Simple Network Management Protocol), IPMI (Intelligent Platform Management Interface), JMX (Java Management Extensions) e monitoramento de ambientes virtualizados, como o VMware. Além disso, o Zabbix permite a criação de verificações personalizadas que podem ser configuradas com intervalos específicos ou agendadas para momentos exatos. Essas verificações podem ser executadas pelo servidor central, por proxies ou por agentes instalados nos dispositivos monitorados (Zabbix SIA, 2024a).

2.5.1.2.2 Definição de Limites Flexíveis

No Zabbix, os limites flexíveis são conhecidos como *triggers* e referenciam os valores armazenados no banco de dados da monitoração. Esses limites são definidos para acionar alertas automaticamente quando certos parâmetros, como a utilização de CPU ou memória, ultrapassam os valores pré-determinados (Zabbix SIA, 2024a).

2.5.1.2.3 Alertas Altamente Configuráveis

O sistema de notificações do Zabbix é altamente configurável. O envio de alertas pode ser ajustado de acordo com o tipo de mídia, seja e-mail, SMS ou aplicativos de mensagens, e com escalonamento de destinatários, garantindo que as notificações sejam enviadas a diferentes responsáveis conforme a necessidade. Além disso, as notificações podem se valer de macros (variáveis que inserem informações dinâmicas nas mensagens) e incluir comandos remotos automáticos, que são executados sem intervenção manual, como reiniciar serviços (Zabbix SIA, 2024a).

2.5.1.2.4 Gráficos Sob Demanda (Em Tempo Real)

Qualquer item numérico armazenado pelo Zabbix pode ser utilizado para a geração de gráficos sob demanda, permitindo visualização em tempo real. Isso elimina a necessidade de planejamento anterior para a criação de gráficos, oferecendo flexibilidade na análise de dados (Zabbix SIA, 2024a).

2.5.1.2.5 Capacidades de Monitoramento de Sites (Web Monitoring)

O Zabbix também inclui capacidades de monitoramento de sites, onde pode simular uma sequência de passos em uma página da web para verificar sua funcionalidade e medir o tempo de resposta. Este recurso é essencial para garantir a disponibilidade e a eficiência dos serviços web (Zabbix SIA, 2024a).

2.5.1.2.6 Diversas Opções de Visualização

O Zabbix permite a criação de gráficos personalizados que combinam vários itens de monitoramento em uma única apresentação visual. Além disso, a plataforma suporta a criação de mapas de rede interativos, telas customizadas e apresentações de slides, que facilitam a visualização em painéis de controle. Também oferece relatórios detalhados e visões de alto nível, permitindo que as empresas acompanhem a saúde dos recursos monitorados de forma estratégica (Zabbix SIA, 2024a).

2.5.1.2.7 Histórico e Armazenamento de Dados

Os dados coletados pelo Zabbix são armazenados em um banco de dados, e o histórico de coleta pode ser configurado de acordo com as necessidades da organização. O sistema possui um processo interno para limpeza de dados antigos,

evitando o acúmulo excessivo de informações e otimizando o uso de espaço (Zabbix SIA, 2024a).

2.5.1.2.8 Configuração Simplificada

No Zabbix, todos os dispositivos ou serviços monitorados são chamados de *hosts*. A solução permite que os hosts sejam monitorados automaticamente assim que inseridos no banco de monitoramento. Além disso, perfis de monitoramento, conhecidos como *templates*, podem ser aplicados aos dispositivos, o que simplifica a configuração e a manutenção das verificações (Zabbix SIA, 2024a).

2.5.1.2.9 Uso de Templates

Os *templates* agrupam várias verificações em um único perfil que pode ser aplicado a diferentes hosts. Esses templates podem herdar propriedades de outros templates, permitindo uma configuração eficiente e escalável (Zabbix SIA, 2024a).

2.5.1.2.10 Descoberta de Rede

O Zabbix oferece mecanismos de descoberta automática de dispositivos na rede, o que facilita a inclusão de novos equipamentos no ambiente monitorado. O sistema também suporta o registro automático de agentes, permitindo que os dispositivos registrem automaticamente sua presença no servidor de monitoramento.

Além disso, há suporte para a autodescoberta de componentes internos, como sistemas de arquivos e interfaces de rede (Zabbix SIA, 2024a).

2.5.1.2.11 Interface Web Ágil

A interface web do Zabbix, desenvolvida em PHP, é acessível de qualquer local via navegador. A plataforma oferece facilidade de navegação, com a possibilidade de visualizar logs de auditoria que registram todas as alterações feitas no sistema, garantindo a rastreabilidade das ações (Zabbix SIA, 2024a).

2.5.1.2.12 API Zabbix

A API do Zabbix fornece uma interface programável que facilita a automação e a integração com outras ferramentas. Isso permite a realização de atualizações em massa, além de possibilitar a integração com ferramentas de terceiros, ampliando as capacidades de monitoração e controle (Zabbix SIA, 2024a).

2.5.1.2.13 Sistema de Permissões

O Zabbix oferece um sistema robusto de permissões, com autenticação segura dos usuários. Determinados usuários podem ser restringidos a visualizar apenas subconjuntos de funções e hosts, garantindo a segurança e a privacidade das informações monitoradas (Zabbix SIA, 2024a).

2.5.1.2.14 Arquitetura de Agente Totalmente Expansível

Os agentes do Zabbix, instalados nos dispositivos monitorados (hosts), são compatíveis com os sistemas operacionais Windows e Linux. Esses agentes são responsáveis por coletar e enviar dados ao servidor central, e sua arquitetura expansível permite a adição de novos recursos conforme necessário (Zabbix SIA, 2024a).

2.5.1.2.15 Binários da Solução (Daemons)

Os daemons do Zabbix, componentes centrais que executam as operações de monitoração, são escritos em C, garantindo alto desempenho e baixo consumo de memória. Além disso, a portabilidade desses daemons facilita a adaptação do Zabbix em diferentes ambientes (Zabbix SIA, 2024a).

2.5.1.2.16 Pronto para Ambientes Complexos

A monitoração remota em ambientes complexos é facilmente gerenciada com o uso de proxies Zabbix, que atuam como intermediários na coleta de dados em locais remotos, enviando essas informações ao servidor central de forma segura e eficiente (Zabbix SIA, 2024a).

2.5.1.3 Template

No Zabbix, um *template* é definido como um conjunto de entidades que pode ser facilmente vinculado a vários hosts, incluindo itens, *triggers*, gráficos, aplicações, telas, regras de descoberta automática e cenários web (Zabbix SIA, 2024a). O uso de *templates* simplifica o monitoramento, eliminando a necessidade de configurar

manualmente cada host. Ao associar um *template* a um host, o Zabbix automaticamente replica o perfil de monitoramento necessário.

A principal razão para usar *templates* é a eficiência e a padronização. Se você está monitorando muitos hosts ou aplicações idênticas ou similares, os *templates* garantem que todos recebam a mesma configuração, sem inconsistências ou erros manuais. Além disso, como mencionado, "qualquer alteração necessária, como adicionar uma nova métrica de monitoração, pode ser feita diretamente no template, e todos os hosts associados serão automaticamente atualizados" (Zabbix SIA, 2024a). Isso permite que alterações sejam centralizadas e aplicadas de forma rápida e eficiente, tornando os *templates* uma ferramenta essencial para reduzir o esforço administrativo e garantir monitoramento confiável.

2.5.1.4 Avaliação da ferramenta

Considerando sua estrutura e funcionalidades, a utilidade do Zabbix no contexto corporativo e acadêmico torna-se ainda mais evidente. Sua capacidade de prevenir falhas sistêmicas através do monitoramento proativo, identificar e resolver problemas antes que impactem o usuário final, e otimizar recursos de infraestrutura através de uma análise detalhada de desempenho, são fatores que contribuem diretamente para a estabilidade e segurança das operações. Dessa forma, o Zabbix oferece uma base sólida para a tomada de decisões estratégicas em relação à infraestrutura de TI, assegurando a continuidade das operações e a eficiência organizacional (Janssen, 2020).

Embora o Zabbix se destaque como uma ferramenta robusta e amplamente utilizada para o monitoramento de infraestruturas de TI, existem outras ferramentas no mercado que compartilham características e funcionalidades semelhantes, como Nagios, Icinga e Prometheus. A seguir, serão apresentadas algumas dessas ferramentas, para oferecer uma visão comparativa, permitindo identificar qual solução atende melhor às necessidades específicas de diferentes infraestruturas. Essa análise possibilita avaliar as vantagens e limitações de cada ferramenta no monitoramento eficaz de redes, servidores e aplicações, garantindo uma gestão otimizada dos recursos tecnológicos.

2.5.2 Nagios

O Nagios, que foi originalmente chamado de Netsaint, foi desenvolvido por Ethan Galstad e uma equipe de mais de 150 desenvolvedores espalhados pelo mundo. Esta equipe se dedica a diversas atividades, incluindo a criação de plugins, a correção de erros, o desenvolvimento da interface web e a produção de documentação abrangente, além da tradução de conteúdo. O software é distribuído gratuitamente sob a licença GPL, o Nagios Core, o que permite sua utilização e modificação livremente e também possui a versão paga, o Nagios XI, versão mais recente. Embora tenha sido projetado para atender a grandes ambientes, sua eficácia em redes menores é notável, permitindo a detecção de quedas de serviços ou de hosts monitorados (Nagios Enterprises LLC, 2024).

A eficácia do Nagios no monitoramento de redes é ampliada pela utilização de plugins, que podem ser escritos em CGI ou em outras linguagens interpretáveis. Isso permite que programadores de diferentes origens contribuam com extensões. O site oficial do Nagios (www.nagios.org) disponibiliza uma variedade de plugins que complementam suas funcionalidades.

2.5.2.1 Funcionamento Básico

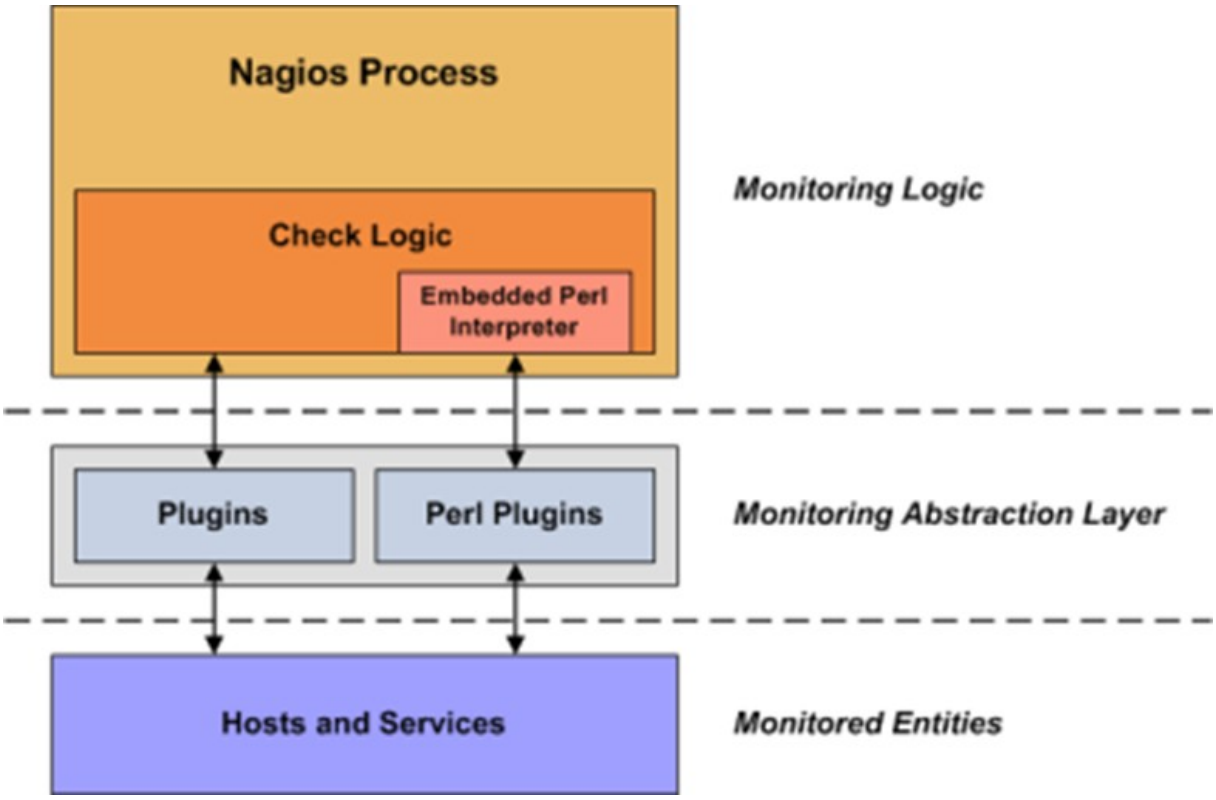
O Nagios Core executará um plugin sempre que houver necessidade de verificar o status de um serviço ou host. O plugin executa uma ação para realizar a verificação e, em seguida, simplesmente retorna os resultados para o Nagios Core. O Nagios Core processará os resultados que receber do plugin e tomará as ações necessárias (Nagios Enterprises LLC, 2018).

Os plugins atuam como uma camada de abstração entre a lógica de monitoramento presente no Nagios Core e os serviços e hosts reais que estão sendo monitorados, conforme a figura 4. A vantagem deste tipo de arquitetura de plugin é que se pode monitorar praticamente qualquer coisa que se possa pensar.

Se for possível automatizar o processo de verificação de algo, ele poderá ser monitorado com o Nagios Core. Já existem muitos plugins que foram criados para monitorar recursos básicos, como carga do processador, uso do disco, taxas de ping, etc (Nagios Enterprises LLC, 2018).

A desvantagem desse tipo de arquitetura de plugins é o fato de que o Nagios Core não tem absolutamente nenhuma ideia do que está monitorando. É possível monitorar estatísticas de tráfego de rede, taxas de erro de dados, temperatura ambiente, tensão da CPU, velocidade do ventilador, carga do processador, espaço em disco. O Nagios Core não entende as especificidades do que está sendo monitorado, ele apenas rastreia as alterações no estado desses recursos. Somente os próprios plugins sabem exatamente o que estão monitorando e como realizar as verificações reais (Nagios Enterprises LLC, 2018).

Figura 4: Plugins Como Camada de Abstração



Fonte: Nagios Enterprise LLC, 2018

Embora tenha sido desenvolvido inicialmente para funcionar em sistemas Linux, o Nagios também é compatível com várias versões do UNIX, como FreeBSD, OpenBSD e NetBSD. Além disso, o Nagios possui a capacidade de identificar

problemas em hosts monitorados por meio de plugins externos, que são gerenciados pelo daemon. Quando um problema é detectado, o sistema pode notificar o administrador ou contatos designados através de diversos meios, incluindo e-mails, mensagens instantâneas, SMS e outras soluções que podem ser desenvolvidas. Além de notificações, conforme a figura 5 o Nagios fornece informações sobre o status dos sistemas, histórico de logs e permite a definição de quais usuários terão acesso visual às informações por meio da interface web (Nagios Enterprises LLC, 2014).

Figura 5: Dashbord do Nagios

Fonte: Nagios Enterprise LLC, 2014

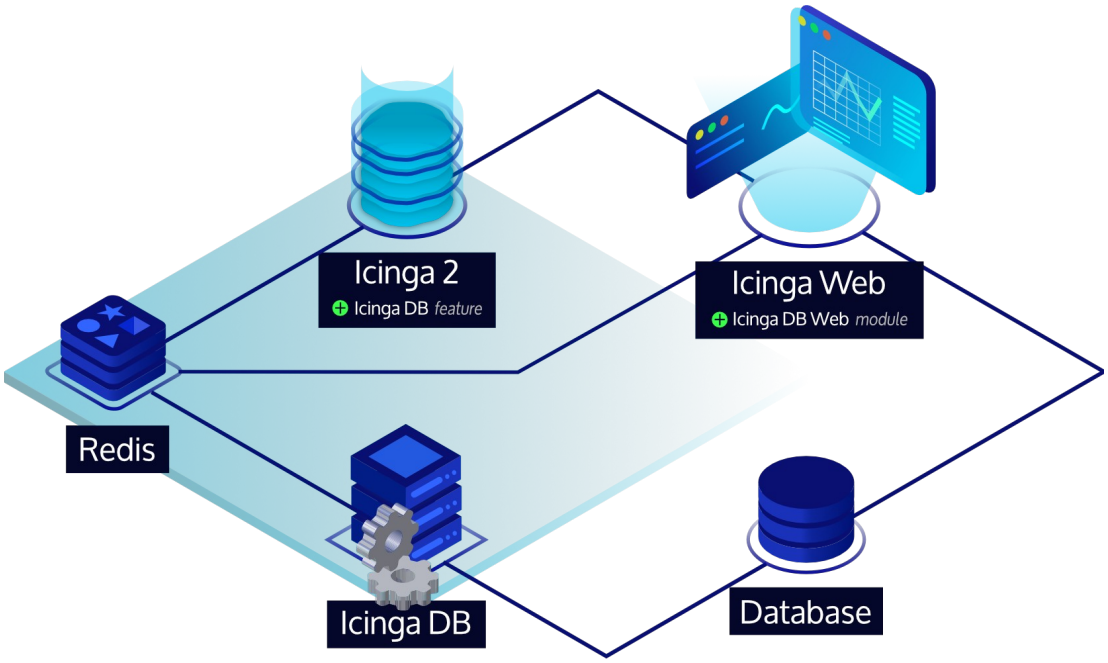
2.5.3 Icinga

O Icinga é uma solução *open-source* altamente flexível, projetada para monitorar uma ampla gama de dispositivos e serviços, como redes, impressoras, *switches*, roteadores, sensores de temperatura, além de serviços locais ou acessíveis via rede. Ele também oferece monitoramento de nuvens privadas, públicas ou híbridas dentro de um data center, com suporte para hosts individuais ou

grupos de hosts, proporcionando escalabilidade para diferentes tamanhos de infraestrutura (Icinga GmbH, 2024).

A figura 6 ilustra os principais componentes do Icinga. O Icinga 2 publica dados no servidor Redis, um acrônimo de REmote DIctionary Server (servidor de dicionário remoto), enquanto o Icinga DB sincroniza essas informações com o banco de dados, garantindo alta disponibilidade e suporte a configurações distribuídas em *clusters*. O Icinga Web facilita a visualização desses dados por meio de *dashboards* intuitivos, permitindo o monitoramento eficiente e a análise do desempenho da rede e dos serviços (Icinga GmbH, 2024).

Figura 6: Ecossistema Icinga



Fonte: Icinga GmbH, 2024

As notificações são uma parte fundamental do sistema de monitoramento. O Icinga 2 permite a configuração de notificações para informar os administradores sobre problemas de serviço ou host, como inatividade, falhas reconhecidas ou inacessibilidade, determinada por sua lógica de dependência. Além disso, o sistema permite a aplicação de filtros de tipo e estado para refinar quais notificações serão enviadas, garantindo que apenas as mensagens relevantes cheguem aos destinatários (Icinga GmbH, 2024).

Embora o Icinga 2 não tenha suporte oficial e não seja recomendado para ambientes de produção, ele oferece mecanismos prontos para notificações via e-mail, Rocket.Chat e webhook. Há também suporte para uma variedade de outros canais de comunicação, como XMPP, IRC e Twitter. Entretanto, o Icinga 2 não realiza o envio das notificações diretamente, dependendo de mecanismos externos, como *scripts* de shell, para notificar os usuários (Icinga GmbH, 2024).

A configuração das notificações exige a definição de um ou mais usuários, ou grupos de usuários, que serão alertados em caso de problemas. Esses usuários devem ter atributos personalizados previamente definidos, os quais serão utilizados pelo comando de notificação *NotificationCommand* no momento da execução. Isso oferece flexibilidade na escolha dos canais de comunicação e permite a personalização das notificações de acordo com as necessidades da organização (Icinga GmbH, 2024).

2.5.4 Prometheus

O software Prometheus é uma ferramenta de monitoramento e alerta de código aberto, inicialmente desenvolvida pela SoundCloud em 2012. Desde então, sua popularidade cresceu, sendo adotada por diversas empresas e organizações. Atualmente, o Prometheus é mantido por uma comunidade ativa de desenvolvedores e usuários, operando de forma independente.

O Prometheus coleta e guarda informações de desempenho ao longo do tempo, registrando cada dado com a data e hora em que foi obtido. Além disso, essas informações podem ter etiquetas adicionais para facilitar a identificação. Algumas das principais características do Prometheus são:

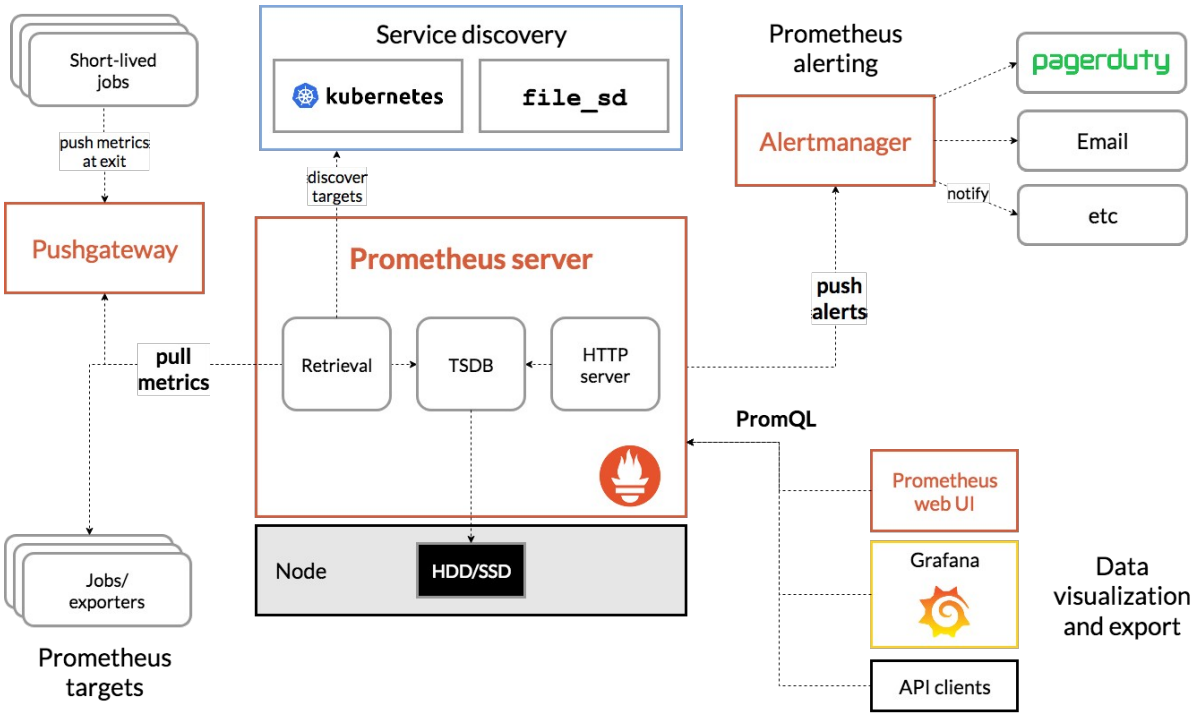
- **Modelo Pull de Coleta**: O Prometheus coleta dados ao fazer solicitações pela internet, "puxando" as informações dos sistemas que está monitorando.
- **Descoberta de Serviços**: Os destinos podem ser descobertos através de mecanismos de descoberta de serviços ou configuração estática.
- **Suporte a Gráficos e Paineis**: A ferramenta oferece várias opções para visualização de métricas, facilitando a análise dos dados.

Conforme exposto acima, a ferramenta faz uso intenso de métricas, que, em termos simples, referem-se a medidas numéricas que ajudam a monitorar o desempenho de um aplicativo. Já a noção de séries temporais se refere ao registro de mudanças ao longo do tempo. O que se deseja medir pode variar conforme a aplicação; por exemplo, em um servidor web, as métricas podem incluir tempos de resposta de requisições, enquanto em um banco de dados, pode-se monitorar o número de conexões ativas ou consultas em execução.

Essas métricas são essenciais para entender o comportamento de um aplicativo. Por exemplo, se um aplicativo web estiver apresentando lentidão, métricas como contagem de solicitações podem indicar que um aumento na carga está causando o problema. Com esses dados, é possível tomar decisões informadas, como aumentar o número de servidores para melhorar a capacidade de resposta (PROMETHEUS Authors, 2024).

Portanto, Prometheus é eficiente para registrar qualquer tipo de dado numérico ao longo do tempo. Ele é adequado tanto para monitoramento de máquinas quanto para arquiteturas baseadas em serviços. Em ambientes de microsserviços, sua capacidade de coletar e consultar dados multidimensionais é especialmente vantajosa. Além disso, o Prometheus foi projetado para ser confiável, permitindo diagnosticar problemas rapidamente durante uma falha. Cada servidor Prometheus funciona de forma independente, sem depender de armazenamento em rede ou serviços externos. De acordo com a figura 7, isso significa que podemos contar com ele mesmo quando outras partes da sua infraestrutura não estão funcionando, e não há a necessidade de configurar uma estrutura complexa para utilizá-lo (PROMETHEUS Authors, 2024).

Figura 7: Arquitetura Prometheus



Fonte: Prometheus Authors, 2024

2.5.5 GLPI

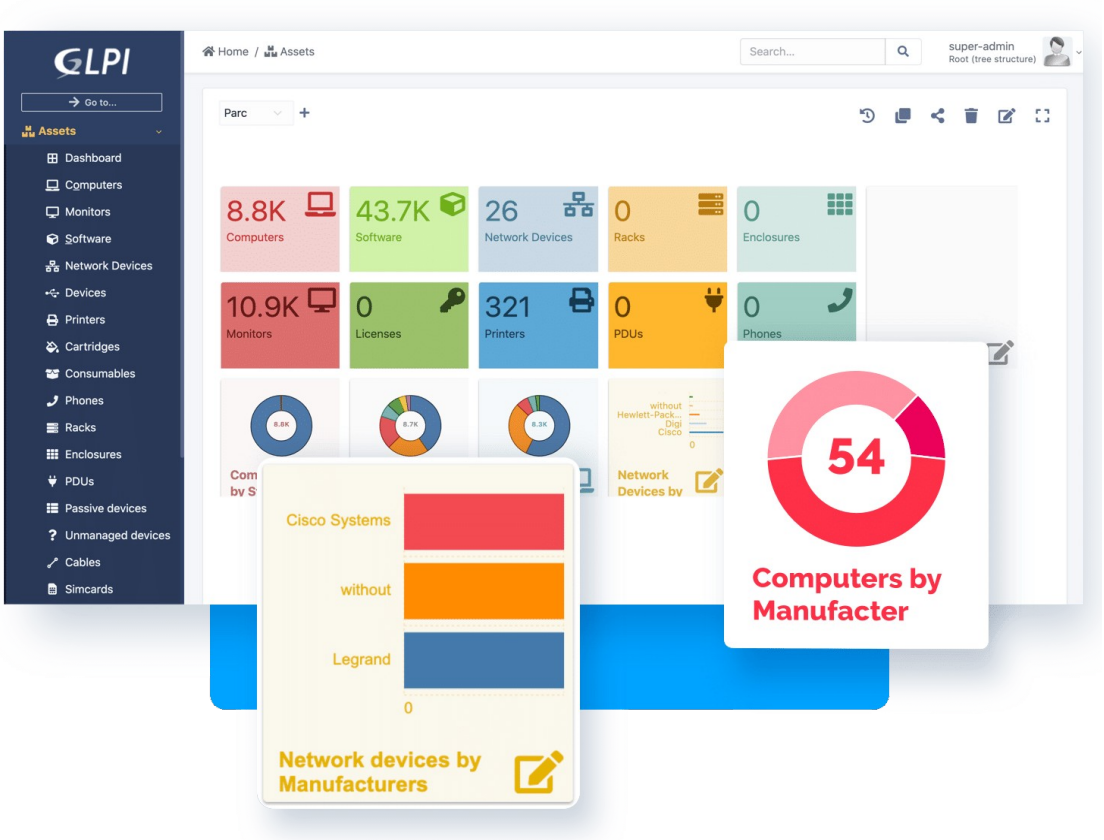
O GLPI é um sistema de código aberto, com foco principal na gestão de serviços e no gerenciamento de ativos de TI. Segundo a GLPI Brasil (2024), a plataforma possibilita a criação de uma "Central de Serviços" completa, reunindo o gerenciamento de incidentes, requisições, projetos, ativos e uma variedade de relatórios e gráficos em uma única ferramenta.

Em uma análise mais aprofundada, o sistema oferece uma ampla e flexível gama de relatórios, que facilitam a identificação rápida e eficaz de chamados, requisições, projetos e equipamentos que necessitam de atenção. Isso permite que os chamados mais críticos sejam visualizados de forma ágil em um único relatório, auxiliando na identificação de áreas, analistas e ativos de melhor e pior desempenho, além de promover a implementação de melhores práticas. Tudo isso é

realizado por meio de plugins e integração com ferramentas de monitoramento mais robustas, bem como a gestão de assistência aos usuários.

O GLPI utiliza, entre outros, o plugin FusionInventory para realizar monitoramento em tempo real, gerenciando inventário, descobrindo redes e agendando tarefas, incluindo o *Wake-on-LAN*[3] e o gerenciamento de dispositivos desconhecidos (Duriuex, 2022). Quando um computador está em modo de suspensão ou desligado, ele pode ser ativado enviando um pacote especial de dados chamado *magic packet*. Para uma visão mais completa, podem ser utilizados plugins que mostram os dados em *dashboard*, permitindo a visualização de gráficos, estatísticas e relatórios, conforme a figura 8, além de ser útil para gerenciamento de chamados (Donato, 2021).

Figura 8: Dashboard do GLPI



Fonte: GLPI Copyright © 2015-2024 Teclib, 2024

O GLPI é escalável principalmente em gerenciamento de inventário, mas necessita de integração para monitorar sistemas complexos. Possui um sistema de

[3] Funcionalidade que permite ligar computadores remotamente pela rede.

notificações por e-mail e pode ser personalizado com plugins para outras formas de notificação. Há também a possibilidade de, após a integração com Zabbix, os alertas gerados no Zabbix serem enviados ao GLPI criando chamados de cada alerta (Zabbix SIA, 2024b).

Outra característica fundamental do GLPI é sua capacidade de monitorar também softwares, o que permite às organizações controlar e monitorar os programas instalados em sua infraestrutura de TI, tornando simples a gestão de licenças, que comumente é um desafio em repartições públicas e garantindo que a organização esteja em conformidade com as políticas de uso, evitando multas e ou notificações por uso indevido de determinado software (GLPI Copyright © 2015-2024 Teclib, 2024).

2.5.6 PRTG

Alguns usuários de sistemas de TI enfrentam dificuldades para aproveitar plenamente as funcionalidades de uma ferramenta, muitas vezes exigindo orientação e estudo intenso para utilizá-la de forma eficaz. Esse desafio reflete a usabilidade, um indicador de qualidade na engenharia de software. O P*aessler Router Traffic Grapher* (PRTG) é uma ferramenta que considera esse aspecto. (Comé, 2023; Paessler GmBh, 2024).

O PRTG é uma solução abrangente para o monitoramento e mapeamento de redes, e-mails, arquivos e servidores, incluindo ambientes virtuais (Paessler GmBh, 2024). Seu valor vai além da simples vigilância, pois oferece a capacidade de entender e responder a incidentes de forma eficaz. Através de painéis dinâmicos, o PRTG exibe dados em tempo real, mostrando desempenho ao vivo e informações de status. (Miracle, 2024). Esses painéis podem ser personalizados com uma variedade de elementos e também permitem a integração de componentes externos, proporcionando uma visão completa da infraestrutura monitorada.

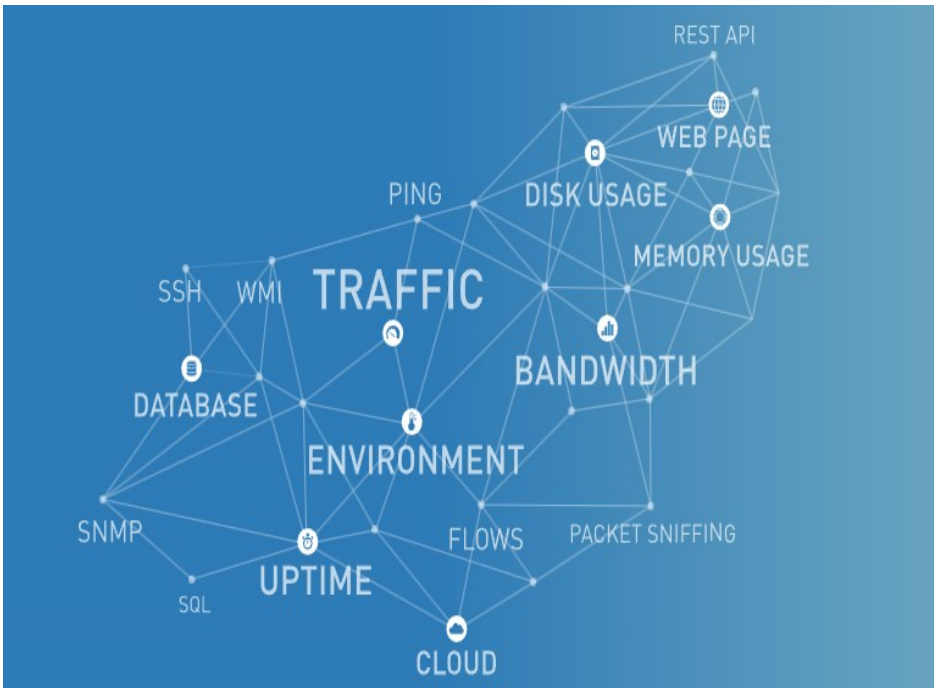
Além de ser intuitivo, o PRTG oferece uma ampla gama de opções de notificação para alertar os administradores sobre a disponibilidade da rede. As notificações são automáticas e podem ser configuradas previamente. O usuário apenas precisa definir informações como número de telefone, e-mail e login,

podendo usar um gatilho para especificar quando deseja receber alertas sobre a disponibilidade ou criticidade do dispositivo. As opções de notificação incluem WhatsApp, e-mail, SMS, gravação em log, mensagens SNMP, AWS, Microsoft Teams, dentre outros (Paessler GmBh, 2024).

É importante destacar que o PRTG não é uma ferramenta gratuita e está disponível apenas para sistemas Windows. No entanto, pode ser utilizado em outros sistemas sem instalação, por meio do PRTG Monitor acessado via navegador web. Outra característica relevante do PRTG é a aplicação do conceito de herança do modelo orientado a objetos, que estabelece uma estrutura hierárquica onde elementos superiores influenciam os subordinados, enquanto a definição dos itens subordinados não afeta os superiores.

A estrutura hierárquica do PRTG, conforme a figura 9, é organizada da seguinte forma: o root é o item de maior superioridade, seguido por sondas, grupos, dispositivos e sensores. O monitoramento é realizado pelas sondas, que podem ser locais, remotas, de cluster ou hospedadas, organizando os dispositivos ou grupos de dispositivos a serem monitorados.

Figura 9: Estrutura hierárquica do PRTG



Fonte: Paessler GmbH, 2024.

Dispositivos podem ser facilmente adicionados através do painel principal, utilizando um plugin na parte superior direita da tela, representado por um ícone de soma. Muitos dispositivos podem ser adicionados informando apenas o endereço IP. Durante a criação de um dispositivo, o sistema pode adicionar automaticamente sensores que buscam os dados mais relevantes. Além disso, é possível definir sensores personalizados conforme as necessidades do usuário (Paessler GmBh, 2024).

2.5.7 Análise Comparativa das Ferramentas

Embora ferramentas como Zabbix, Nagios, Icinga, Prometheus, GLPI e PRTG compartilhem muitas funcionalidades essenciais, como monitoramento de infraestrutura em tempo real, geração de alertas e visualização de métricas, cada uma delas possui características que as tornam mais adequadas para diferentes cenários.

O Zabbix se destaca por sua interface amigável e extensa capacidade de integração, sendo ideal para organizações que buscam uma solução completa para monitoramento de infraestrutura de TI. Sua flexibilidade e arquitetura modular permitem monitorar uma vasta gama de dispositivos, aplicações e serviços.

Por outro lado, Nagios e Icinga são opções robustas e amplamente configuráveis, especialmente recomendadas para usuários que já têm familiaridade com a comunidade Nagios. Essas ferramentas se diferenciam pela flexibilidade na criação de *plugins* e pela capacidade de monitorar de forma personalizada redes e serviços. Icinga, em particular, é projetado para escalabilidade e integração com novas tecnologias de comunicação.

O GLPI, embora ofereça funcionalidades básicas de monitoramento, é amplamente utilizado no gerenciamento de ativos de TI e no suporte ao usuário,

permitindo o controle detalhado de inventário e a criação de chamados para atendimento técnico, sendo uma escolha comum em ambientes de TI voltados à gestão de serviços e infraestrutura.

Para cenários mais modernos, especialmente aqueles que envolvem microsserviços e arquitetura em nuvem, o Prometheus se destaca como a melhor escolha. Sua abordagem para monitoramento e análise de séries temporais é altamente eficiente, proporcionando visibilidade detalhada de métricas e permitindo diagnósticos rápidos em ambientes dinâmicos.

Por fim, o PRTG foca na usabilidade, sendo uma ferramenta amigável tanto para iniciantes quanto para usuários avançados. Ele oferece uma experiência simples e intuitiva, ideal para organizações que priorizam facilidade de uso sem abrir mão da robustez no monitoramento de redes, servidores e ambientes virtuais.

A escolha da ferramenta de monitoramento mais adequada depende das necessidades específicas do ambiente em questão. Enquanto o Zabbix é uma solução abrangente e o Prometheus brilha em ambientes de microsserviços, Nagios e Icinga são ótimos para personalização e flexibilidade. O GLPI se destaca na gestão de serviços e ativos de TI, e o PRTG se sobressai pela sua facilidade de uso, tornando o processo de monitoramento acessível a todos. Para ilustrar melhor os aspectos específicos de cada ferramenta e suas funcionalidades, o Quadro 2 apresenta um comparativo que destaca as principais características e vantagens de cada uma. Esse quadro oferece uma visão clara e objetiva, facilitando a análise das ferramentas de monitoramento e suas aplicações em diferentes cenários.

Quadro 2: Resumo das características das ferramentas

	Zabbix	**Nagios**	**Icinga**	**Prometheus**	**GLPI**	**PRTG**
Open-Source	Atende totalmente	Atende parcialmente	Atende totalmente	Atende totalmente	Atende totalmente	não atende
Ativos que monitora	Servidores, dispositivos de rede, serviços de aplicação, máquinas virtuais e sistemas operacionais	Servidores, dispositivos de rede, aplicações, serviços e logs	Servidores, dispositivos de rede, serviços, sistemas operacionais e contêineres	Microserviços, contêineres, serviços web, aplicações	Ativos de TI, Incidentes, Documentação	Servidores, Dispositivos de rede, aplicações, tráfego de rede, Máquinas virtuais
Escalabilidade	Atende totalmente	Atende parcialmente	Atende totalmente	Atende totalmente	Atende parcialmente	Atende parcialmente
Alertas	Atende totalmente	Atende totalmente	Atende parcialmente	Atende totalmente	Atende totalmente	Atende totalmente
Dashboards	Múltiplos e personalizáveis	simples	personalizáveis.	Integrado com grafana	personalizáveis	personalizáveis
Dados Históricos	atende totalmente	não atende	atende parcialmente	atende totalmente	atende totalmente	atende totalmente
Gerenciamento de	atende totalmente	atende totalmente	atende totalmente	atende totalmente	atende totalmente	atende totalmente

Configurações						
Alta Disponibilidade	atende totalmente	atende parcialmente	atende totalmente	atende totalmente	atende parcialmente	atende totalmente
Integração	atende totalmente	atende totalmente	atende totalmente	atende totalmente	atende totalmente	atende totalmente

Fonte: O autor

Observados os diversos critérios citados no quadro 2, destacam-se como ferramentas mais aderentes o Zabbix e o Prometheus. Contudo, comparando-se as duas, observa-se que o Zabbix se adequa melhor a infraestrutura que suporta os serviços que serão monitorados no modelo proposto.

2.6 GRAFANA

Software de código aberto grafana permite consultar, visualizar, alertar e explorar métricas, logs e rastreamentos onde quer que estejam armazenados. O Grafana *Open Source Software* (OSS) fornece ferramentas para transformar seus dados de banco de dados de séries temporais (TSDB) em gráficos e visualizações perspicazes (Grafana Labs, 2024).

É possível integrar o Zabbix com Grafana sendo uma prática comum para criar *dashboards* detalhados que mostram dados de monitoramento em tempo real. Uma das principais vantagens dessa integração é a visualização intuitiva, permitindo que as métricas sejam visualizadas de forma mais clara e compreensível do que apenas com o Zabbix (Grafana Labs, 2024).

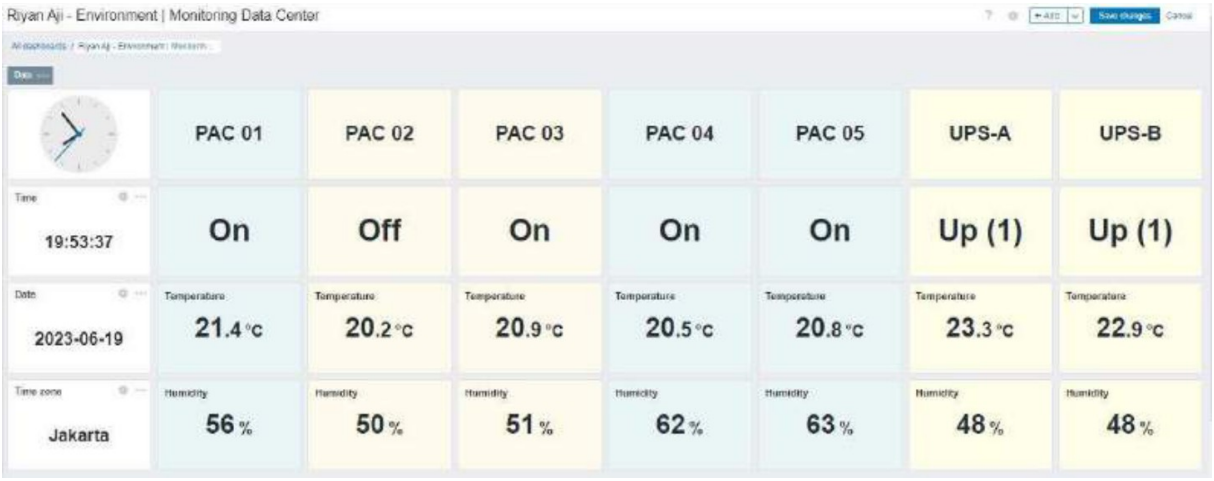
Além disso, o Grafana permite a criação de alertas personalizados. Embora o Zabbix tenha suas próprias funcionalidades de alerta, o Grafana pode complementar isso, oferecendo alertas baseados em visualizações complexas e condições específicas configuradas no *dashboard*.

Por fim, o Grafana oferece flexibilidade e customização. É possível aplicar filtros, ajustar intervalos de tempo e personalizar praticamente todos os aspectos da visualização. Isso oferece uma maior flexibilidade para atender às necessidades específicas de monitoramento, tornando a integração com o Zabbix ainda mais eficaz (Grafana Labs, 2024).

2.7 TRABALHOS RELACIONADOS

Com o objetivo de avaliar a disponibilidade e a confiabilidade dos servidores, Nugroho e Rosyani (2023) realizaram um estudo utilizando o Zabbix para monitorar seu data center, com ênfase em parâmetros como umidade, temperatura e quedas de energia. Os autores observaram que, em redes de grande porte, a identificação de problemas pode ser bastante desafiadora. Nesse contexto, eles concluíram que um sistema de monitoramento torna a detecção de falhas mais eficiente e rápida, permitindo identificar rapidamente a temperatura e a umidade de vários servidores, como mostrado na figura 10.

Figura 10: Painel com monitoramento da temperatura e umidade



Fonte: Nugroho; Rosyani, 2023

Comé (2023) realizou um trabalho de campo na empresa ALTEL, que administra a rede de computadores da Meridian32. Anteriormente, a empresa utilizava um monitoramento manual por meio de logs, resolvendo anomalias de serviço apenas após sua ocorrência. Contudo, Comé (2023) buscou uma solução que permitisse a detecção proativa de falhas, visando garantir uma maior disponibilidade dos serviços.

Após avaliar diversas ferramentas de monitoramento, dentre elas, PRTG, Nagios, Zabbix e Cacti[4], decidiu implementar o Zabbix, o que possibilitou o

2

4 É uma ferramenta open-source com foco no monitoramento do tráfego da rede (Comé, 2023).

monitoramento de roteadores, *switches*, *Access Points (AP) e Network Video Recorders* (NVR). Para aumentar a agilidade na resposta a incidentes, optou por notificar os administradores por e-mail, evitando que problemas se agravassem e elevando a capacidade estratégica no monitoramento do sistema.

Lijó (2022) também aborda a dificuldade enfrentada pelos técnicos quando se deslocam para realizar correções devido à indisponibilidade de serviço, que pode ser agravada pela localização geográfica. O estudo ressalta a importância de utilizar uma ferramenta de monitoramento para identificar possíveis falhas e quedas de serviço. Entre as falhas citadas estão o rompimento de cabos, interferência elétrica ou climática. Além disso, Lijó (2022) prevê a crescente utilização de ferramentas automatizadas de monitoramento para otimizar a detecção e a gestão desses problemas.

Por fim, Reis (2021) adotou os conceitos da ITIL para aprimorar o monitoramento de falhas na empresa Koerich Engenharia, que enfrentava dificuldades devido a um processo de monitoramento mal definido, sem resolução automática e com alta dependência de intervenção humana. Para propor uma solução, Reis (2021) seguiu as etapas do gerenciamento de eventos da ITIL e realizou uma análise comparativa entre as ferramentas Zabbix, Datadog[5], Elastic Stack[6] e Sentry[7]. Ele optou pela implementação do Zabbix e Sentry, pois essas ferramentas oferecem maior precisão na comunicação das falhas e maior utilidade para as partes interessadas.

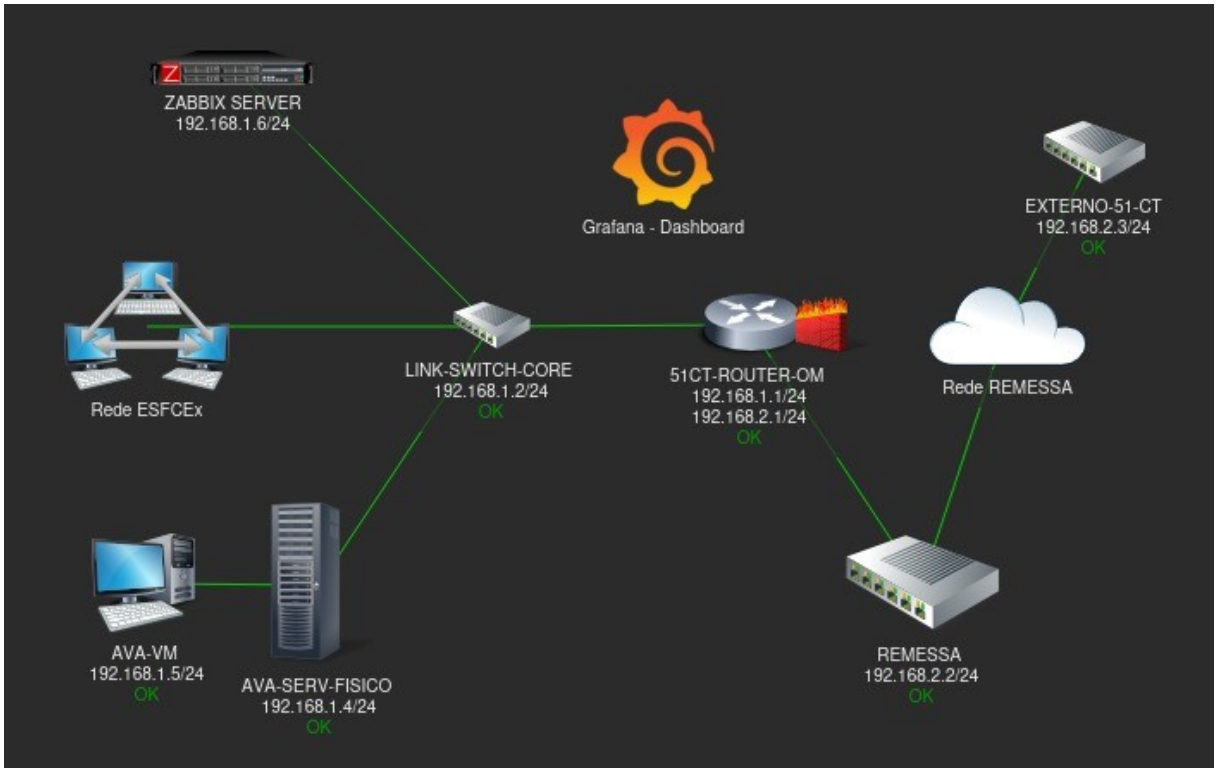
3. RESULTADOS

Os resultados apresentados a seguir foram obtidos a partir de simulações realizadas no ambiente de rede monitorado pela ferramenta Zabbix (Figura 11), com foco nas métricas previamente estabelecidas. As simulações incidiram sobre as

[5] Ferramenta que não é open-source e serve para monitoramento de servidores, banco de dados, ferramentas e serviços. (Reis, 2021).
[6] Ferramenta open-source para busca e visualização de dados (Reis, 2021)
[7] Ferramenta open-source para monitoramento de erros em aplicações (Reis, 2021).
3
4
5

métricas de latência, largura de banda e disponibilidade da rede, visando avaliar o desempenho do serviço em operação sobre a infraestrutura de rede em diferentes condições operacionais.

Figura 11: Mapa da rede utilizada para o estudo de caso.



Fonte: O autor.

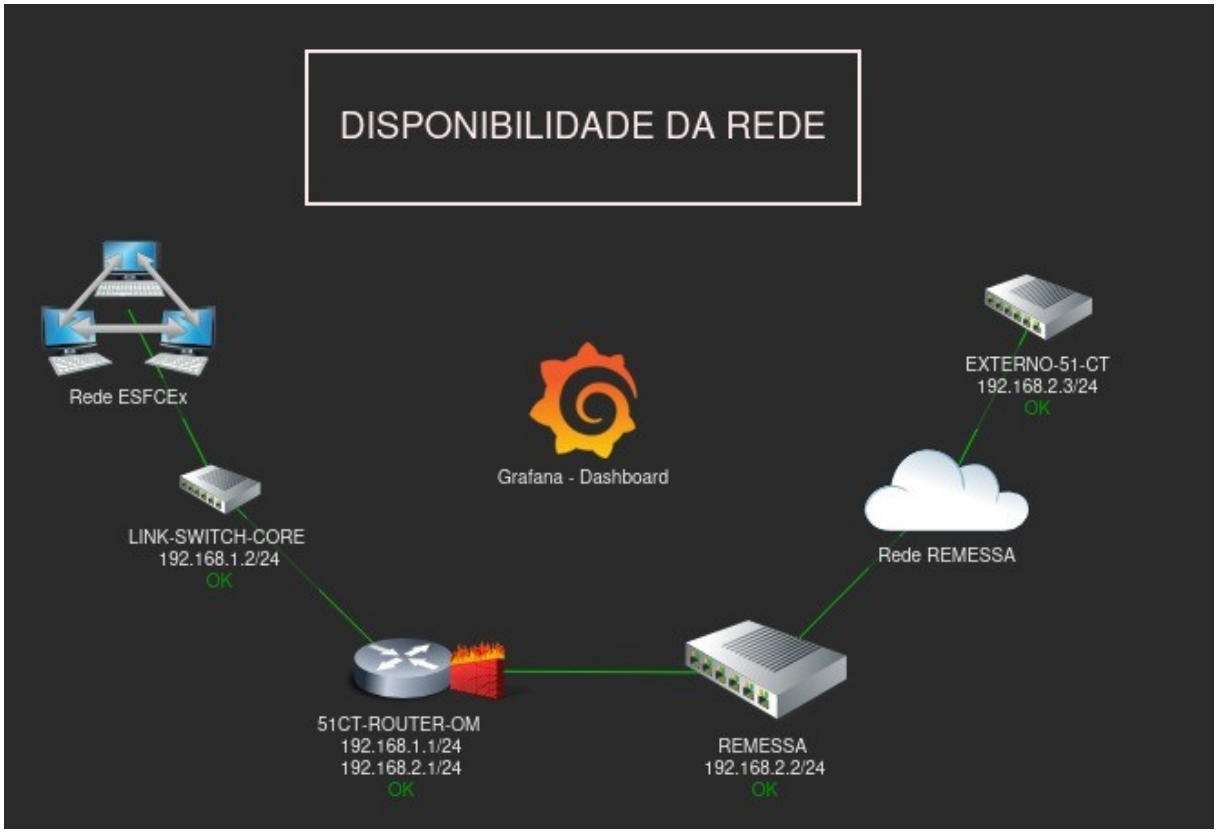
3.1. Simulação de monitoramento - link de Internet

Nesta seção, serão descritos os diferentes cenários avaliados no decorrer do estudo, com ênfase exclusiva na análise da disponibilidade do serviço de internet. Cada cenário foi estruturado com base em condições operacionais específicas, com o objetivo de simular situações que podem influenciar a continuidade dos serviços. Os dados apresentados por meio dos mapas de monitoramento, gerados pelo Zabbix, são utilizados para avaliar a disponibilidade dos dispositivos da rede em cada cenário. A apresentação detalhada de cada cenário permitirá uma avaliação do

comportamento do serviço sobre a infraestrutura em termos de disponibilidade, oferecendo subsídios para a análise crítica dos resultados.

A Figura 12 apresenta o cenário geral de disponibilidade da rede da ESFCEx, onde são exibidos os principais dispositivos conectados. A visualização inclui dispositivos como o LINK-SWITCH-CORE, 51CT-ROUTER-OM, REMESSA, e o EXTERNO-51-CT, todos operando com o status "OK", que se encontra abaixo do IP. Essa representação oferece uma visão global da infraestrutura da rede, permitindo o monitoramento da disponibilidade de cada dispositivo em tempo real.

Figura 12: Mapa do estudo de caso do link de internet.



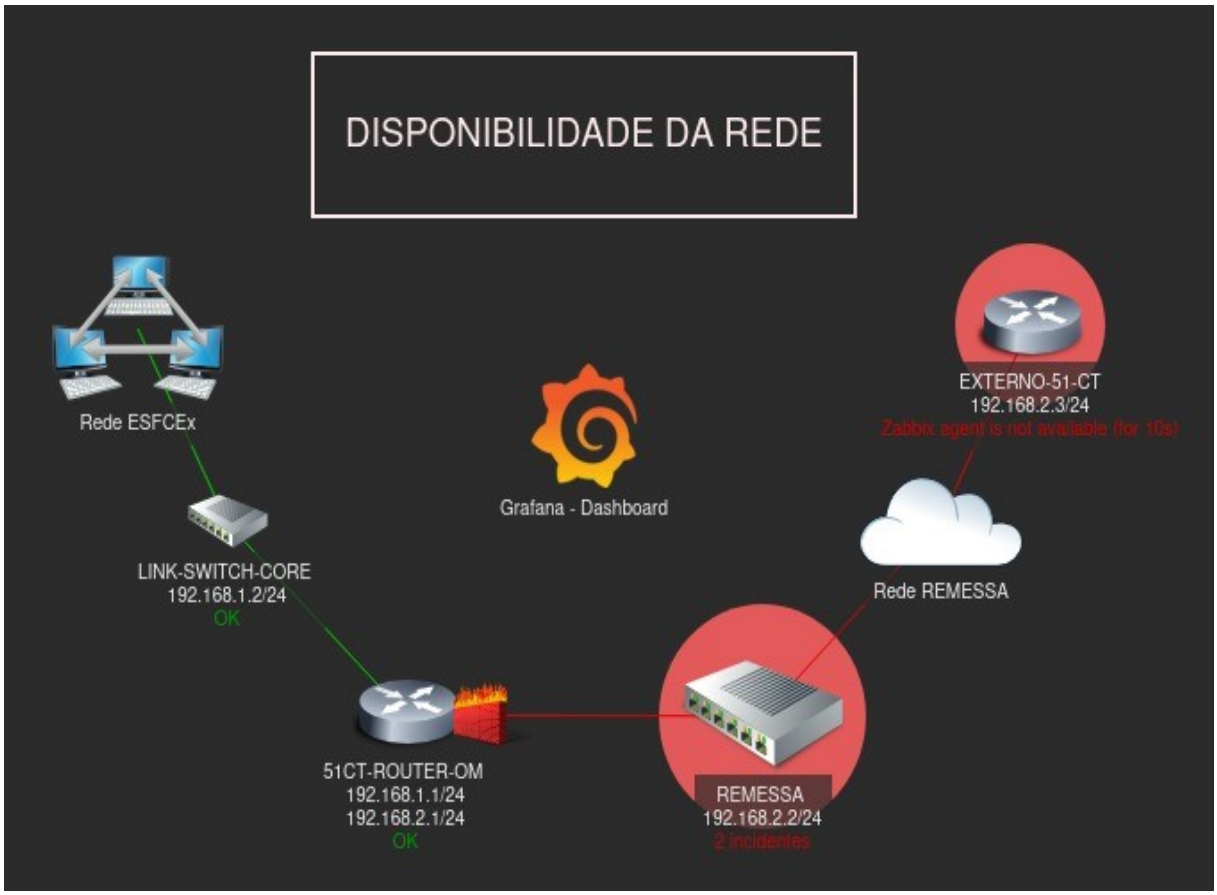
Fonte: O autor.

3.1.1. Simulação 1 - Remessa

Na Figura 13, pode-se observar que os dispositivos 51CT-ROUTER-OM (192.168.1.1/24 - 192.168.2.1/24), LINK-SWITCH-CORE (192.168.1.2/24)

encontram-se em pleno funcionamento, conforme indicado pelo status "OK". Entretanto, o dispositivo REMESSA (192.168.2.2/24), principal elemento no fornecimento de acesso à internet para toda a rede, está indisponível, conforme sinalizado pela mensagem "Zabbix agent is not available (for 10s)". Como consequência dessa falha, o dispositivo EXTERNO-51-CT (192.168.2.3/24) também se tornou inacessível, já que o tráfego de rede desta passa diretamente pela REMESSA.

Figura 13: Indisponibilidade da REMESSA



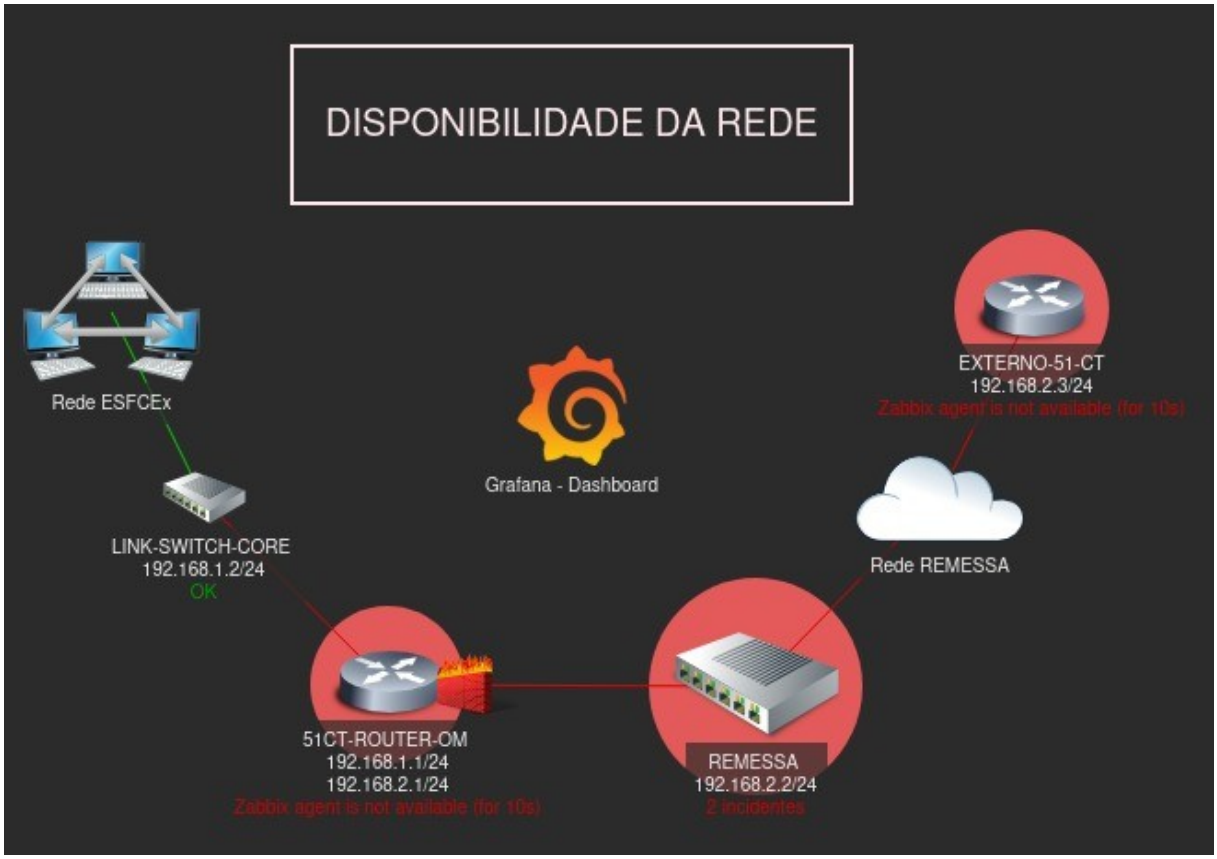
Fonte: O autor.

3.1.2. Simulação 2 - 51CT-ROUTER-OM

Na Figura 14, o dispositivo 51CT-ROUTER-OM (192.168.1.1/24 - 192.168.2.1/24) encontra-se indisponível, conforme indicado pela mensagem

"Zabbix agent is not available (for 10s)", sinalizando que o agente de monitoramento Zabbix não conseguiu se comunicar com esse dispositivo. Devido à queda do 51CT-ROUTER-OM, o status do EXTERNO-51-CT (192.168.2.3/24) não pode ser verificado, uma vez que o tráfego de rede desta passa pelo 51CT-ROUTER-OM. Dessa forma, o EXTERNO-51-CT assume o mesmo status de indisponibilidade do 51CT-ROUTER-OM.

Figura 14: Indisponibilidade do 51CT-ROUTER-OM



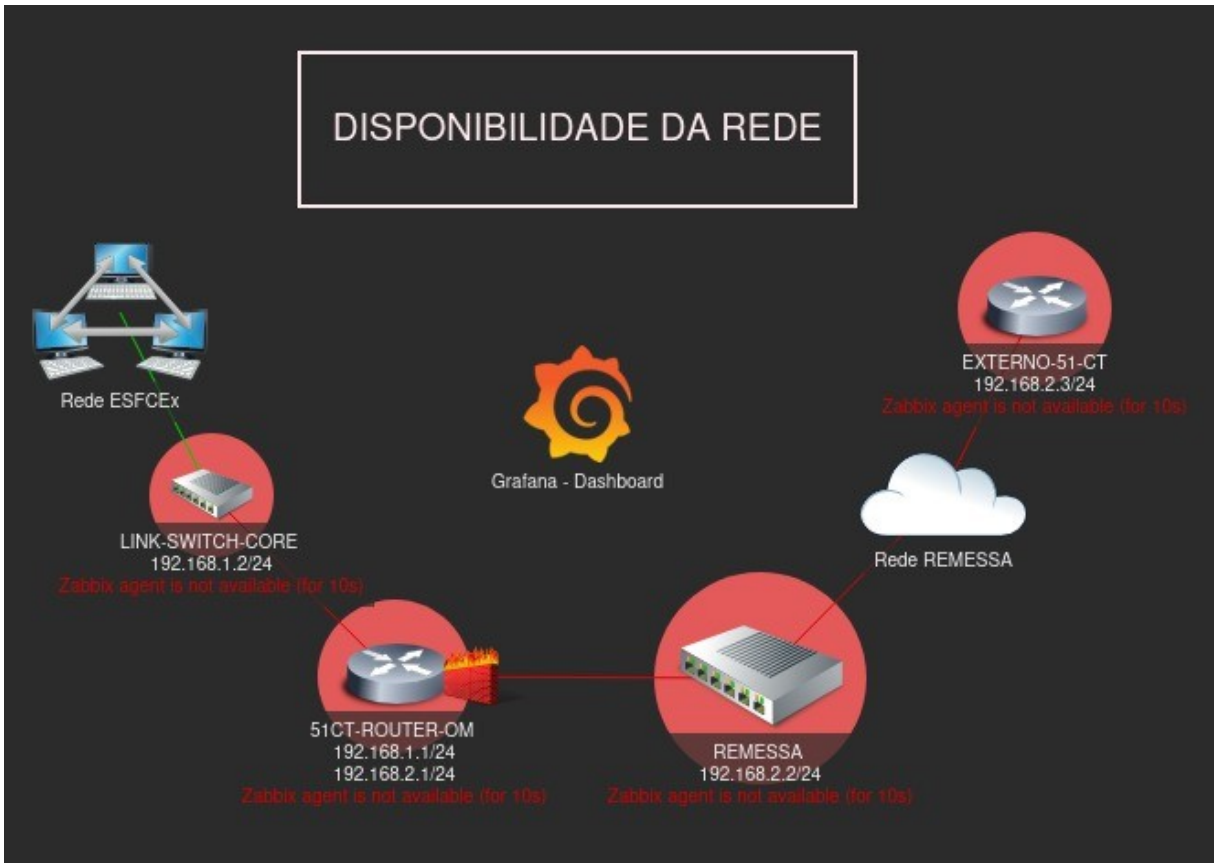
Fonte: O autor.

3.1.3. Simulação 4 - Switch Core

Na Figura 15, o LINK-SWITCH-CORE (192.168.1.2/24) está fora de operação. Uma vez que o Zabbix está ligado ao LINK-SWITCH-CORE, a REMESSA (192.168.2.2/24), 51CT-ROUTER-OM (192.168.1.1/24 - 192.168.2.1/24) e

EXTERNO-51-CT (192.168.2.3/24) também ficam com o status de indisponibilidade no mapa.

Figura 15: Indisponibilidade do Switch Core



Fonte: O autor.

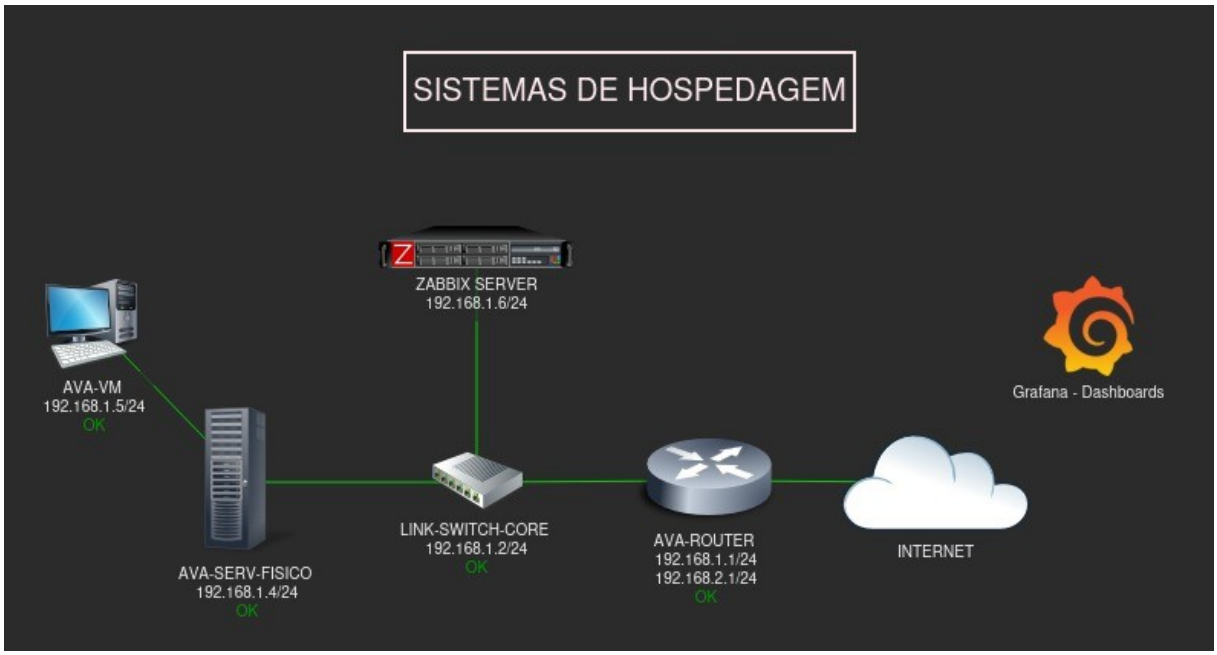
3.2. Simulação de monitoramento - Sistema de hospedagem

Esta seção apresenta os resultados obtidos na simulação da disponibilidade do serviço de hospedagem ao sistema AVA, seguindo a mesma abordagem descrita na análise do serviço de internet. Os cenários apresentados são baseados em condições operacionais específicas que podem afetar a continuidade do AVA, permitindo avaliar como o sistema se comporta em diferentes situações. Assim como no item anterior, a apresentação detalhada de cada cenário permitiu uma visão clara do comportamento do sistema em termos de disponibilidade.

A Figura 16 apresenta o monitoramento do serviço de hospedagem do AVA. Nessa visualização, são exibidos os principais dispositivos que compõem a

infraestrutura de hospedagem, incluindo a AVA-VM, o AVA-SERV-FISICO, LINK-SWITCH-CORE e o AVA-ROUTER, todos operando com o status "OK".

Figura 16: Mapa do estudo de caso do sistema de hospedagem

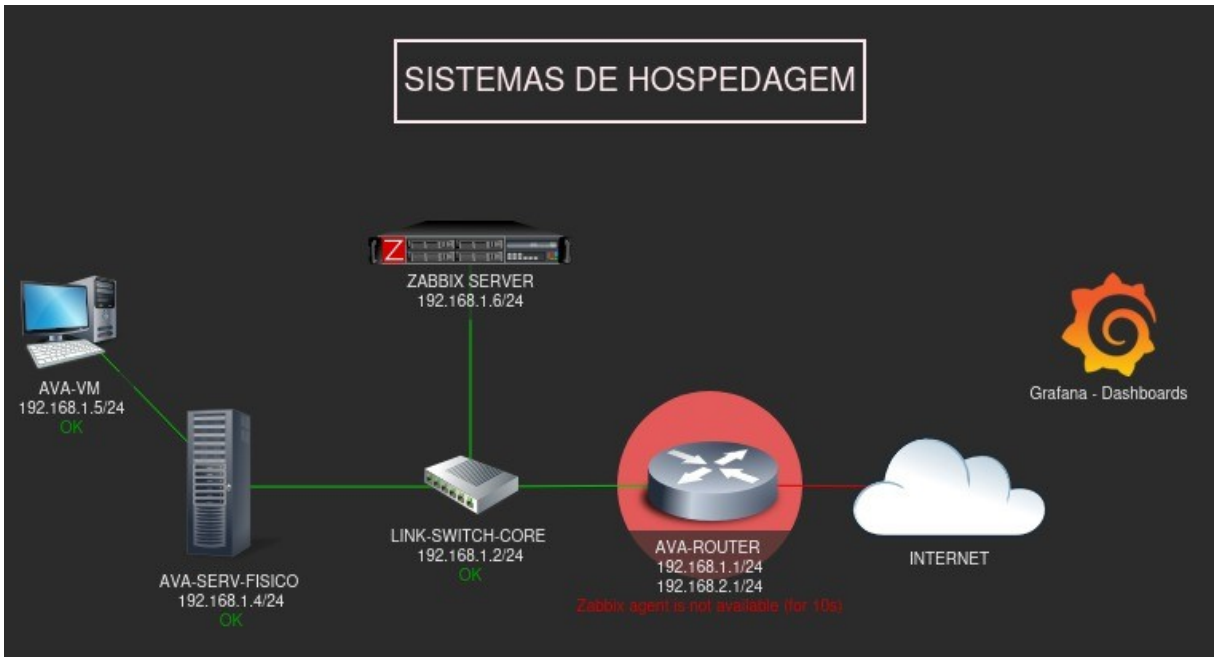


Fonte: O autor.

3.2.1. Simulação 1 – Indisponibilidade do AVA-ROUTER

Na Figura 17, pode-se observar que o dispositivo AVA-ROUTER encontra-se indisponível, indicando dois incidentes. Apesar disso, o LINK-SWITCH-CORE, AVA-SERV-FISICO e o AVA-VM se encontram com status “OK”, apresentado abaixo do IP.

Figura 17: Indisponibilidade do AVA-ROUTER

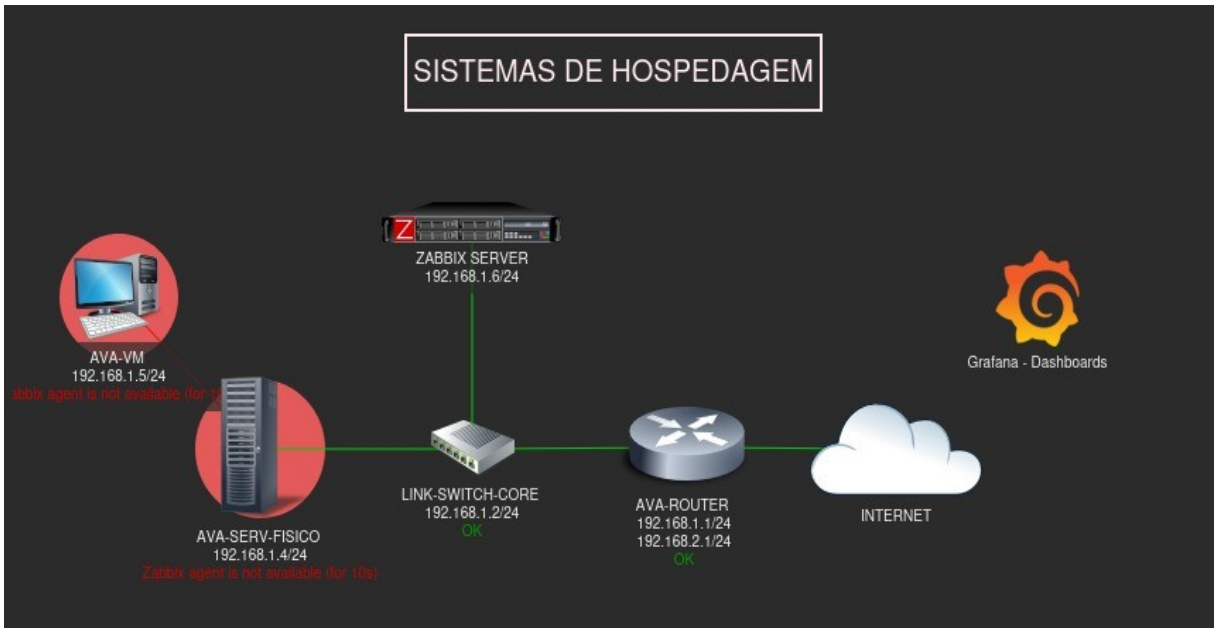


Fonte: O autor.

3.2.2. Simulação 2 - Indisponibilidade do AVA-SERV-FISICO

Na figura 18, pode-se observar que os dispositivos AVA-ROUTER e LINK-SWITCH-CORE encontram-se em pleno funcionamento, conforme indicado pelo status "OK". Entretanto, o dispositivo AVA-SERV-FISICO, responsável pela hospedagem do AVA, está indisponível, conforme sinalizado pela mensagem "Zabbix agent is not available (for 10s)", assim como o dispositivo AVA-VM também se encontra indisponível.

Figura 18: Indisponibilidade do AVA-SERV-FISICO

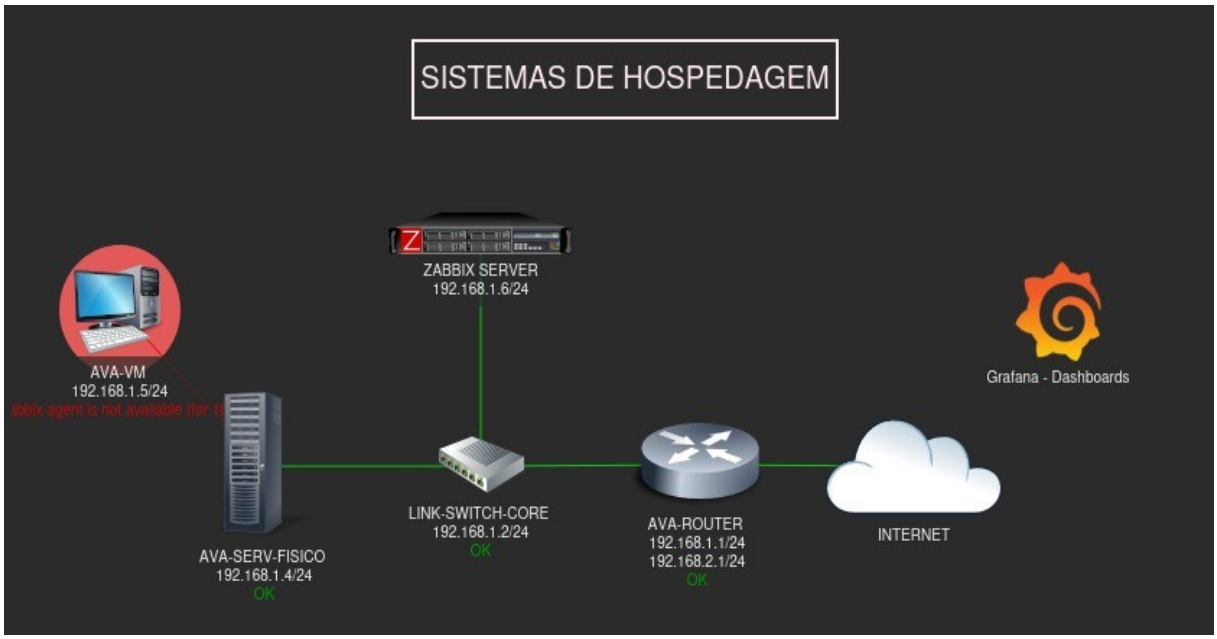


Fonte: O autor.

3.2.3. Simulação 3 - Indisponibilidade do AVA-VM

Na Figura 19, pode-se observar que os dispositivos AVA-ROUTER, LINK-SWITCH-CORE e AVA-SERV-FISICO encontram-se em pleno funcionamento, conforme indicado pelo status "OK". Entretanto, o dispositivo AVA-VM está indisponível, conforme sinalizado pela mensagem "Zabbix agent is not available (for 10s)".

Figura 19: Indisponibilidade do AVA-VM

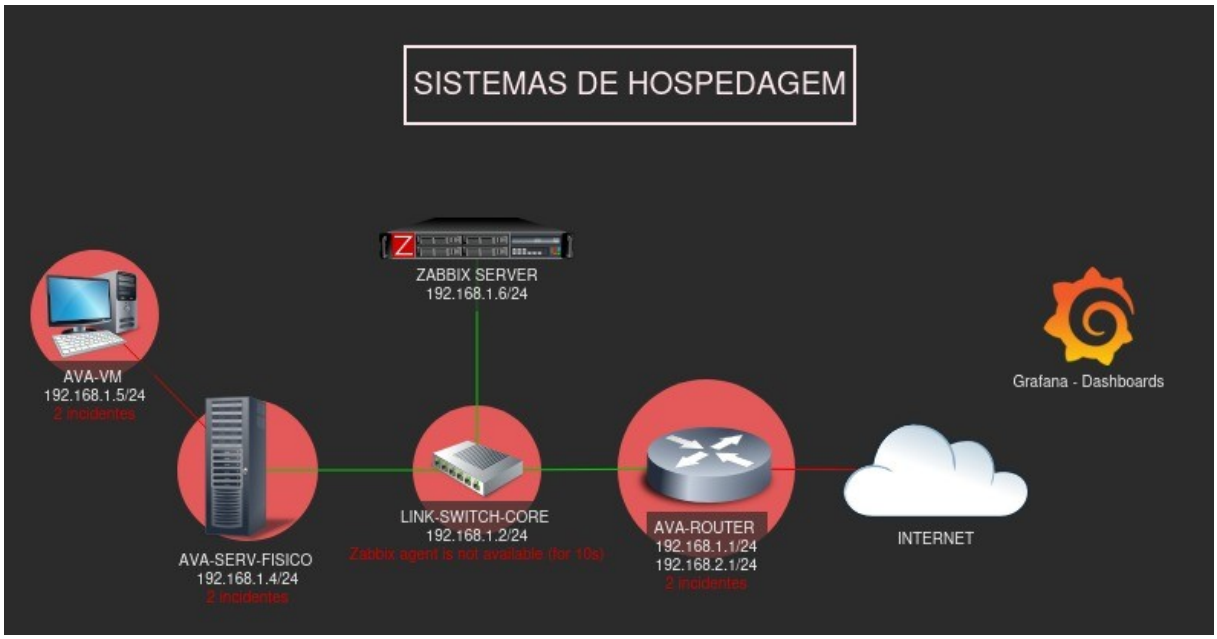


Fonte: O autor.

3.2.4. Simulação 4 - Indisponibilidade do LINK-SWITCH-CORE

Na Figura 20, o LINK-SWITCH-CORE está indisponível, como consequência disso, os dispositivos AVA-VM, o AVA-SERV-FISICO e o AVA-ROUTER ficam inacessíveis, fazendo com que seu status também seja de indiponivilidade.

Figura 20: Indisponibilidade do AVA-VM



Fonte: O autor.

3.3. Dados Dashboard do Grafana

Esta seção apresenta os dados coletados na simulação pelo Zabbix e exibidos por meio das *dashboards* criadas no Grafana, apresentado no item 2.4, organizadas em dois cenários distintos apresentados respectivamente nas seções 4.3.1 e 4.3.2. Cada *dashboard* oferece uma visão detalhada dos principais parâmetros de desempenho da infraestrutura de rede e do AVA. As informações foram organizadas de forma a permitir uma análise clara e objetiva do comportamento dos sistemas monitorados em cada cenário, tanto o link de internet, quanto o sistema de hospedagem, facilitando a compreensão de sua disponibilidade e desempenho.

3.3.1 Link de Internet

A Figura 21 contém o dashboard que apresenta o monitoramento do link de internet, exibindo informações relacionadas as métricas “Capacidade” e “Disponibilidade”, conforme descrito nas seções 4.3.1.1 e 4.3.1.2.

Figura 21: Dashboad criado no Grafana para monitoramento do Link de Internet

Fonte: O autor.

3.3.1.1 Capacidade

Tempo de resposta (ICMP): No canto superior esquerdo do painel, é mostrado o tempo de resposta em microssegundos (µs) via ICMP, indicando as variações ao longo de 5 horas e meia. A linha verde representa o tempo de resposta, com picos acima de 210 µs e quedas até 155 µs, o que sugere momentos de maior latência na rede.

Largura de banda (bits enviados x bits recebidos): No canto superior direito, o painel mostra o tráfego de rede em bits enviados e recebidos. A linha amarela (banda recebida) fica abaixo de 200 kb/s, e a linha verde (banda enviada)

tem picos até 700 kb/s. Esses valores indicam que a utilização de largura de banda é moderada, longe dos limites críticos, mantendo a rede sem saturação.

3.3.1.2 Disponibilidade

A seção inferior da dashboard mostra o status de disponibilidade do link, indicado como "Up" (quadro “Status”), junto com o tempo de atividade acumulado (quadro “Tempo de atividade”) Já a seção denominada “**incidentes**” apresenta eventos registrados, com informações sobre o host afetado, a severidade do incidente, o status e o tipo de problema, além do horário do ocorrido.

3.3.2 Serviço de hospedagem - AVA

A Figura 22 apresenta as métricas de monitoramento da máquina virtual do AVA, hospedada em um servidor, destacando informações de “Capacidade” e “Disponibilidade”, conforme descrito nas seções 4.3.2.1 e 4.3.2.2.

Figura 22: Dashboad criado no Grafana para monitoramento do AVA

Fonte: O autor.

3.3.2.1 Capacidade

Armazenamento Disco: Localizado no canto superior esquerdo da *dashboard*, o painel apresenta o percentual de utilização do disco, indicando que 3,19% do espaço total disponível está ocupado. Esse valor reflete a quantidade de dados armazenados em relação à capacidade total do sistema.

Uso de Memória: Localizado no centro superior da dashboard, o painel exibe o uso de memória, mostrando que 37,9% da memória total está em uso. O painel também detalha a quantidade de memória livre e utilizada, com um total de 3,82 GiB de memória disponível e 2,37 GiB atualmente em uso.

Uso de CPU: Localizado no canto superior direito da dashboard, o painel apresenta o uso da CPU, indicando que 13,8% da capacidade de processamento está em uso no momento. Este valor reflete a carga atual sobre o processador.

Tempo de resposta: Localizado no canto inferior esquerdo da dashboard, o painel exibe o tempo de resposta medido em microssegundos (µs) via ICMP. Ele mostra as variações no período de 05 horas e meia, simulando o acesso de um usuário ao longo do período monitorado, permitindo a visualização das latências observadas nas comunicações entre o sistema e os hosts conectados. Observa-se a variação da resposta ICMP ao longo do tempo. A linha verde, que representa o tempo de resposta, apresenta oscilações com picos que ultrapassam 210 µs e quedas que chegam a 150 µs. Isso demonstra flutuações de desempenho que podem afetar a experiência do usuário.

Largura de banda (bits enviados x bits recebidos): Localizado no canto inferior direito da *dashboard*, o painel apresenta o tráfego de rede em termos de bits enviados e bits recebidos ao longo do tempo. Ele permite acompanhar a utilização da largura de banda, distinguindo claramente entre o volume de dados transmitidos e recebidos pela rede. Nota-se que o valor da banda recebida (linha amarela) permanece abaixo de 500 kb/s durante grande parte do tempo, enquanto a banda enviada (linha verde) apresenta um comportamento semelhante, com picos que não ultrapassam 700 kb/s. Esses dados indicam que a utilização de largura de banda é moderada, não chegando perto dos limites críticos para a interface monitorada, o que sugere que o tráfego atual está bem abaixo da capacidade máxima suportada, garantindo um funcionamento sem saturação.

3.3.2.2 Disponibilidade

Status: Localizado na parte inferior da dashboard, este painel exibe o status atual do sistema, mostrando o indicador "Up", o que significa que o sistema está operacional e acessível no momento da análise.

Tempo de atividade: Localizado na parte inferior da dashboard, ao lado do painel de status, este painel exibe o tempo total de funcionamento contínuo do sistema. No momento registrado, o sistema acumula 32 dias, 22 horas, 50 minutos e 8 segundos de operação sem interrupções.

3.4 Considerações finais

No capítulo de resultados, foram apresentados os resultados das simulações realizadas de modo a demostrar o funcionamento do modelo proposto conforme as métricas de latência, largura de banda e índice de disponibilidade dos dispositivos monitorados. As informações foram organizadas e exibidas em *dashboards* que demonstram o comportamento da infraestrutura de rede ao longo do período avaliado e suas implicações aos serviços monitorados. A análise detalhada dessas simulações será realizada na seção seguinte, dedicada à discussão.

4. DISCUSSÃO

Após a realização das simulações buscou-se avaliar se o modelo proposto atende as demandas definida no objetivo.

4.1 Análise dos resultados obtidos

A implementação do Zabbix para o monitoramento dos ativos de rede trouxe resultados que demonstram as vantagens da ferramenta na gestão dos serviços do catálogo de serviço do SisTEx conforme o modelo proposto. Entre os principais resultados, destacam-se a coleta de dados sobre a disponibilidade dos serviços, tempo de resposta da rede, uso de CPU e memória, e outros parâmetros importantes para garantir o bom desempenho da infraestrutura. Esses dados foram obtidos de forma contínua, proporcionando uma visão clara e em tempo real do desempenho dos ativos.

Os resultados demostraram que é possível gerir os serviços de Internet e hospedagem de sistema utilizando o modelo implementado na ferramenta. A disponibilidade foi monitorada tanto através dos mapas do Zabbix quanto pelo Grafana, que mostraram o tempo em que os sistemas permaneceram operacionais ("up") de forma visual, oferecendo uma visão clara e detalhada da estabilidade dos serviços.

Além da disponibilidade, outro aspecto importante a ser considerado no monitoramento é a capacidade de armazenamento. A figura 23 ilustra o armazenamento em disco, um aspecto do gerenciamento de capacidade descrito no "Desenho de Serviço" da ITIL. A quantidade de dados armazenados pode impactar o desempenho do sistema, resultando em lentidão.

Figura 23: Armazenamento em Disco

Fonte: O autor.

Adicionalmente, a falta de monitoramento pode levar ao esgotamento dos recursos disponíveis, comprometendo a operação do sistema. Portanto, analisar esse parâmetro é crucial. O gerenciamento de alertas pode utilizar essas informações para notificar o administrador do sistema sobre a quantidade máxima de dados que o sistema pode suportar sem riscos de degradação no desempenho.

Em complemento a isso, o gerenciamento da memória também desempenha um papel vital no desempenho do sistema. A Figura 24 aborda um aspecto crucial relacionado à memória: quando o sistema não possui memória RAM suficiente, ele recorre ao uso de swapping, que é consideravelmente mais lenta, pois utiliza o disco rígido ou SSD para simular RAM adicional.

Figura 24: Uso de Memória

Fonte: O autor.

Esse método pode resultar em uma diminuição significativa na velocidade de acesso e no desempenho geral do sistema. Quando a memória RAM está sobrecarregada e atinge sua capacidade máxima, o sistema começa a trocar dados entre a RAM e o disco rígido. Esse processo, conhecido como *swapping*, pode causar uma lentidão considerável, pois o acesso ao disco rígido ou SSD é muito mais demorado em comparação ao acesso à RAM.

Outro fator indispensável no monitoramento de sistemas é o desempenho da CPU, conforme ilustrado na Figura 25. Sendo um dos componentes mais críticos de uma infraestrutura de TI, a eficiência da CPU tem impacto direto no funcionamento do sistema como um todo. Quando opera em níveis próximos à sua capacidade máxima, há uma tendência de lentidão, especialmente em ambientes onde diversos processos e aplicações são executados simultaneamente, o que torna esse monitoramento ainda mais relevante.

Figura 25: Uso de CPU

Fonte: O autor.

Embora o uso da CPU seja de apenas 2,37%, o monitoramento contínuo dessa métrica é de grande importância. Um percentual tão baixo indica que a capacidade de processamento do sistema está sendo subutilizada neste momento. No entanto, é importante ressaltar que essa situação pode ser temporária e, sob condições de carga variada, o uso da CPU pode aumentar rapidamente. Processos que exigem um alto nível de capacidade de processamento — como aplicações que realizam cálculos complexos, manipulação de grandes volumes de dados ou execução de tarefas intensivas em recursos — podem rapidamente elevar a utilização da CPU, levando a uma competição pelos recursos disponíveis.

Quando isso acontece, outros aplicativos e processos que não estão diretamente relacionados à tarefa intensiva podem sofrer uma queda de desempenho significativa. Essa degradação pode se manifestar na forma de tempos de resposta mais lentos, travamentos ou falhas em processos que dependem de um desempenho ágil da CPU. Assim, mesmo que a utilização atual esteja em um nível aceitável, a capacidade da CPU deve ser monitorada de forma proativa para evitar que a sobrecarga leve à degradação do desempenho do sistema.

Portanto, a análise contínua da utilização da CPU é uma prática recomendada, permitindo que os administradores de sistemas identifiquem

rapidamente quaisquer picos de utilização e implementem ações corretivas, se necessário. Isso pode incluir a otimização de processos, o balanceamento de carga entre diferentes servidores ou, em casos mais extremos, a expansão da capacidade de hardware para garantir que todos os aplicativos operem com eficiência. Em suma, o monitoramento adequado da utilização da CPU é fundamental para manter um desempenho ideal e a confiabilidade do sistema a longo prazo.

Outro aspecto relevante para o desempenho da rede é o tempo de resposta, mostrado na Figura 26. A imagem apresenta os valores monitorados ao longo de um período estipulado, em microssegundos, demonstrando flutuações consistentes, mas dentro de uma faixa controlada, com a maioria dos picos mantendo-se abaixo dos 210 µs. Esses dados refletem uma estabilidade significativa, mesmo durante variações de uso, o que evidencia a capacidade da infraestrutura em lidar com as demandas sem comprometer a qualidade das respostas. Acompanhamentos como esse são fundamentais para garantir que, mesmo em momentos de maior carga, o sistema mantenha seu desempenho dentro de padrões aceitáveis, assegurando a eficiência nas operações e a qualidade da experiência do usuário.

Figura 26: Tempo de Resposta

Fonte: O autor.

O monitoramento do tempo de resposta revelou-se uma métrica essencial para avaliar a eficiência da rede ao longo do período analisado. Os dados indicaram que o sistema manteve respostas consistentemente rápidas, o que reflete a capacidade da infraestrutura em suportar a demanda sem gerar atrasos significativos. A manutenção desse desempenho dentro dos parâmetros estipulados

reforça a confiabilidade do sistema e garante que os serviços críticos sejam entregues de forma eficiente. Essa estabilidade demonstra a eficácia das estratégias de monitoramento adotadas, assegurando que os recursos da rede operem de maneira otimizada, mesmo em momentos de maior carga.

A largura de banda monitorada, conforme ilustrado na Figura 27, revela o comportamento do tráfego de dados ao longo de um período estipulado. O gráfico apresenta a taxa de bits enviados e recebidos, mostrando variações que, na maior parte do tempo, mantêm-se abaixo de 300 kb/s. Durante determinados picos, como por volta das 11:30, observa-se um aumento significativo no tráfego, indicando momentos de maior demanda na rede. Esses picos, apesar de pontuais, permanecem dentro de uma faixa controlada, sem ultrapassar o limite estabelecido de 700 kb/s.

Figura 27: Largura de Banda

Fonte: O autor.

Parâmetros inadequados, como altas taxas de utilização constantes, poderiam sinalizar a necessidade de ampliar a capacidade da rede ou ajustar a alocação de recursos para prevenir gargalos e assegurar a continuidade dos serviços, sobretudo em ambientes críticos que exigem alta disponibilidade.

Um ponto crucial analisado na Figura 28 é o gerenciamento da disponibilidade. O monitoramento contínuo da disponibilidade é de grande importância, pois, quando um site ou serviço fica indisponível, é fundamental que o administrador seja informado de forma imediata. Caso isso não ocorra, os usuários podem ter uma experiência negativa, aguardando a resolução do problema,

enquanto o responsável pelo sistema pode não estar ciente de que o serviço está inativo, aumentando o tempo de inatividade e os impactos negativos.

Figura 28: Status de Disponibilidade

Fonte: O autor.

Durante a simulação de incidentes para análise do monitoramento, foi possível verificar que a ferramenta foi eficiente em destacar os pontos onde ocorreram falhas. Contudo, não foi possível, neste trabalho, identificar a causa raiz dos incidentes observados. Embora a detecção das falhas tenha sido clara, a análise mais profunda sobre suas causas será um tópico para trabalhos futuros, sugerindo que novas investigações serão necessárias para explorar essas origens.

A integração do Zabbix com o Grafana mostrou-se essencial para a visualização dos dados de forma dinâmica e eficiente. As dashboards do Grafana, combinadas com os mapas do Zabbix, facilitaram a compreensão da disponibilidade e desempenho dos serviços, proporcionando uma interface visual intuitiva que auxiliou no monitoramento contínuo.

Em resumo, os resultados obtidos estão alinhados com os objetivos do trabalho, demonstrando que o uso do Zabbix, integrado ao Grafana, foi eficaz no monitoramento da infraestrutura de TI. Isso assegurou alta disponibilidade e desempenho adequado dos sistemas críticos, como o AVA, além de fornecer uma visão clara sobre a disponibilidade dos serviços ao longo do tempo.

4.2. Propostas de trabalhos futuros

Com base nos resultados obtidos e nas observações feitas ao longo deste estudo, surgem oportunidades para aprofundar a pesquisa em áreas específicas. As recomendações para trabalhos futuros visam aprimorar a compreensão dos padrões de uso da rede e a identificação das causas subjacentes às falhas observadas, com o intuito de fortalecer ainda mais a infraestrutura monitorada e otimizar sua performance. Abaixo, serão apresentadas algumas propostas para pesquisas futuras.

Construção de Análise Temporal: Sugere-se, para trabalhos futuros, a construção de uma análise temporal mais detalhada dos dados coletados. Essa abordagem permitirá identificar padrões de utilização da rede ao longo do tempo, oferecendo subsídios para otimizar ainda mais a infraestrutura e prevenir possíveis gargalos de desempenho.

Análise da Causa Raiz das Falhas: Embora este estudo tenha identificado a ocorrência de falhas nos dispositivos monitorados, não foram exploradas as causas subjacentes dessas falhas. Recomenda-se, para pesquisas futuras, a condução de uma análise de causa raiz, com o objetivo de aprimorar a robustez e a confiabilidade da infraestrutura de rede, proporcionando uma melhor capacidade de resposta a incidentes.

5. CONCLUSÃO

A implementação do modelo baseado do ITIL em funcionamento no SisTEx utilizando a ferramenta Zabbix demonstrou ser eficiência na gestão de incidentes e disponibilidade do serviço de Internet e Hospedagem de sistema no âmbito da infraestrutura da ESFCEx. O estudo foi realizado em um ambiente controlado, onde o uso do Zabbix, aliado às práticas da ITIL, possibilitou a detecção falhas, como problemas de conectividade e desempenho de sistemas hospedados.

A análise das métricas de latência, largura de banda e índice de disponibilidade nas simulações demonstrou como o modelo de monitoramento proposto contribuiu para a melhoria da gestão dos serviços oferecidos. Embora em um cenário controlado, as simulações realizadas permitiram identificar de modo ágil os incidentes, contribuindo de forma significa na identificação de potenciais impactos negativos nas operações da OM. O Zabbix, ao fornecer alertas em tempo real e gráficos detalhados por meio do Grafana, garantiu uma visualização clara do status dos ativos e uma rápida intervenção por parte da equipe técnica.

Outro ponto relevante foi a integração com os conceitos da ITIL, que permitiu não apenas o monitoramento dos recursos, mas também a adoção de um modelo de governança com foco no catálogo de serviços do SisTEx.

Além disso, a flexibilidade do Zabbix em se adaptar às necessidades específicas da ESFCEx, reforçou seu papel como uma ferramenta robusta e escalável no monitoramento de infraestrutura de rede. A capacidade de gerar relatórios personalizados, monitorar diferentes componentes e emitir alertas ajustados à criticidade de cada serviço proporcionou benefícios diretos para a equipe de TI, além de contribuir para garantir a continuidade dos serviços essenciais.

Os resultados deste estudo destacam que o modelo adotado, testado em um ambiente controlado, possui potencial para ser aplicado em ambiente de produção e replicado em outras Organizações Militares que enfrentam desafios semelhantes no gerenciamento de suas infraestruturas de TI. No entanto, antes de ser amplamente aplicado, recomenda-se que seja validado em um cenário real específico, onde suas funcionalidades e limitações possam ser avaliadas de forma mais prática. A integração do Zabbix com as práticas de governança da ITIL mostrou-se uma combinação eficaz para garantir alta disponibilidade e segurança dos serviços, tornando-se uma abordagem promissora para instituições que buscam eficiência operacional.

Em suma, conclui-se que a utilização do Zabbix pode trazer melhorias significativas para o controle e monitoramento da infraestrutura de TI na ESFCEx além de servir como um exemplo de como as tecnologias de monitoramento podem ser aplicadas para otimizar processos de gestão em ambientes complexos.

REFERÊNCIAS

AGUIAR, I. F. **Proposta de Utilização da Ferramenta Zabbix no Gerenciamento de Redes**: um Estudo de Caso no Ambiente da FAB Segundo Boas Práticas de Governança de TI. Orientadora: Moacyr Henrique Cruz de Azevedo. Trabalho de Conclusão de Curso (Graduação) – Curso de Ciência da Computação, Universidade Federal do Rio de Janeiro, 2017. Disponível em: https://pantheon.ufrj.br/handle/11422/3300. Acesso em: 14 maio 2024.

AXELOS. **ITIL 4® Foundation:** ITIL 4 Edition. 4. ed. Londres: The Stationery Office, 2019, 209 p. Disponível em: https://www.mizekhedmat.com/wp-content/uploads/2022/07/ITILFoundation-ITIL4Edition.pdf. Acesso em: 14 out. 2024.

BERNARDO. **Monitoramento de Redes com Zabbix**. Disponível em: https://claudiobernard0.wordpress.com/2018/01/25/monitoramento-de-redes-com-zabbix/. Acesso em: 11 out. 2024.

BON, J. V. **ITIL:** Guia de Referência, edição 2011. Tradução: Edson Furmankeiwicz. Rio de Janeiro: Elsevier, 2012. 162 p.

CABINET OFFICE. **ITIL® Service Design.** United Kingdom: The Stationery Office, 2011. 456 p. Disponível em: https://www.kornev-online.net/ITIL/02%20-%20ITIL%20V3%202011%20Service%20Design%20SD.pdf. Acesso em: 14 out. 2024.

CENTRO INTEGRADO DE TELEMÁTICA DO EXÉRCITO. **Catálogo de serviços de TI do SixTEx**: Sistema de Telemática do Exército Conectando o Exército Brasileiro. Brasília: Exército Brasileiro, 2018. Disponível em: https://4cta.eb.mil.br/catalogo/CSTI_SisTEx.pdf. Acesso em: 11 out. 2024.

COMÉ, A. E. **Implementação de um Sistema de Monitoramento de Rede de Computadores na Meridian32.** 2023. 54 f. Monografia (Licenciatura em Engenharia Informática) – Universidade Eduardo Mondlane, Moçambique, 2023. Disponível em: http://monografias.uem.mz/handle/123456789/3262. Acesso em: 17 ago 2024.

COTTA, W. A. A. **Medição de tempo de comunicação e exibição de tempo de resposta para espaços inteligentes programáveis.** 2020. Dissertação (Mestrado em Engenharia Elétrica) - Centro Tecnológico da Universidade Federal do Espírito Santo, Universidade Federal do Espírito Santo, Espírito Santo, 2020. Disponível em: https://sappg.ufes.br/tese_drupal/tese_13368_Dissertacao%20de%20Mestrado%20-%20Wagner%20A.%20A.Cotta%20%28final%29.pdf. Acesso em: 16 out. 2024.

DONATO, S. **Dashboard.** 2021. Disponível em: https://plugins.glpi-project.org/#/plugin/dashboard. Acesso em: 23 ago. 2024.

DUMAN, İ. Ö.; ELİİYİ, U. Performance Metrics and Monitoring Tools for Sustainable Network Management. **Bilişim Teknolojileri Dergis**, v. 14, n. 1, p. 37-51, 2021. Disponível em: https://doi.org/10.17671/gazibtd.780504. Acesso em: 02 set. 2024.

DURIUEX, D. **Fusioninventory for GLPI**. 2022. Disponível em: https://plugins.glpi-project.org/#/plugin/fusioninventory. Acesso em: 23 ago. 2024.

FERREIRA, D. S. S. **Desenvolvimento de um aplicativo para apoiar pessoas com TDAH.** 2023. Trabalho de Conclusão de Curso (Graduação) – Curso de Ciência da Computação, Pontifícia Universidade Católica de Goiás, Goiânia, 2023. Disponível em: https://repositorio.pucgoias.edu.br/jspui/bitstream/123456789/7058/1/TCC%20-%20Douglas%20Soares%20de%20Souza%20Ferreira.pdf. Acesso em: 16 out. 2024.

GLPI Brasil. **O que é GLPI.** 2024. Disponível em: http://www.glpibrasil.com.br/o-que-e-glpi/. Acesso em: 20 out. 2024.

GLPI Copyright © 2015-2024 Teclib. **GLPI Características**: Gerenciamento de TI baseado em Código Aberto. 2024. Disponível em: https://glpi-project.org/pt-br/caracteristicas/. Acesso em: 20 out. 2024.

Grafana Labs. **Technical documentation.** 2024. Disponível em: https://grafana.com/docs/. Acesso em: Acesso em: 23 ago. 2024.

GRIGORIK, I. ITU-T G.107. 1. ed. United States of America: O'Reilly. 2013.

ICINGA GmbH. **Icinga Documentation**. 2024. Disponível em: https://icinga.com/docs/. Acesso em: 12 out. 2024.

JANSSEN. **Monitoramento com Zabbix**. 2. ed. [s.l.]: Brasport, 2020.

KERNITSKYI, Andrii. **What is Good Latency in Networking?** Disponível em: https://obkio.com/blog/what-is-good-latency. Acesso em: out. 28 ago. 2024.

LIJÓ, M. C. **Revisão Sistemática para Monitoramento e Acionamento Elétrico e de Temperatura em Ambiente de Provedor de Internet.** 49 f. 2022. Dissertação (Mestrado em Tecnologia da Informação) - Instituto Federal de Educação, Ciência e Tecnologia da Paraíba, João Pessoa, 2022. Disponível em: https://repositorio.ifpb.edu.br/jspui/handle/177683/2805. Acesso em: 18 ago. 2024.

MINISTÉRIO DA DEFESA; EXÉRCITO BRASILEIRO; SECRETARIA-GERAL DO EXÉRCITO. **Portaria nº 077-Cmt Ex**, de 24 de janeiro de 2019. Aprova o regulamento do Centro Integrado de Telemática do Exército (EB10-R-07.013), 1ª edição, 2019. Brasília: Exército Brasileiro, 2019.

MIRACLE, N. O. The Role of Network Monitoring and Analysis in Ensuring Optimal Network Performance. **International Research Journal of Modernization in Engineering Technology and Science.** v. 6, p. 3009-3025, Nigéria, jun. 2024. Disponível em: https://www.doi.org/10.56726/IRJMETS59269. Acesso em: 09 out. 2024.

Nagios Enterprises LLC. **Nagios Documentation:** Official manuals, documentation, video tutorials, and FAQs for Nagios solutions. 2024. Disponível em: https://nagios.org/documentation. Acesso em: 11 out. 2024.

_____. **Nagios Plugins**. 2018. Disponível em: https://assets.nagios.com /downloads/ nagioscore/docs/nagioscore/4/en/plugins.html. Acesso em: 15 out. 2024.

_____. **Documentation.** 2014. Disponível em: https://nagios-plugins.org/doc. Acesso em: 15 out. 2024.

NUGROHO, R. A.; ROSYANI, P. Implementasi Monitoring Perangkat Environment Menggunakan Zabbix pada Data Center Pusat Data Sarana Informasi (PDSI). **OKTAL**: Jurnal Ilmu Komputer dan Scienc, v. 2, n. 7, p. 1846-1873, Indonesia, jul, 2023. Disponível em: https://journal.mediapublikasi.id/index.php/oktal/article /view/3228/1589. Acesso em: 17 ago. 2024. ISSN: 2828-2442.

Office of Government Commerce. **ITIL Service Strategy.** The Stationery Office, 2007. Disponível em: https://www.kornev-online.net/ITIL/OGC%20-%20ITIL %20v3%20-%20Service%20Strategy.pdf. Acesso em: 1 jun. 2024.

PAESSLER GmBh. **PRTG Manual**: Comprehensive IT monitoring. Nuremberg: 2024. Disponível em: https://manuals.paessler.com/prtgmanual.pdf?_gl=1*880fqp*_gcl_au* MTUzNDk5NTA3MC4xNzIzODUzMTg0*_ga*MTcyMTI2Mjg5MC4xNzIzODUzMTg1*_ ga_JG3ST477CK*MTcyMzg1MzE4NC4xLjEuMTcyMzg1NDE2OC4wLjAuNTU3NzEy MTIy. Acesso em: 16 de ago. 2024.

PROMETHEUS Authors. **Overview:** What is Prometheus? 2024. Disponível em: https://prometheus.io/docs/introduction/overview. Acesso em: 12 out. 2024.

RED HAT, Inc. **O que é open source?** 2024. Disponível em: https://www.redhat.com/pt-br/topics/open-source/what-is-open-source. Acesso em: 11 out. 2024.

REIS, Y. L. S. **Implementando uma Prática de Gerenciamento de Serviços para Rastrear Ocorrência de Falhas do Sistema em Ambiente de Produção**: um Estudo Aplicado a uma Empresa de Prestação de Serviços de Engenharia. 2021. 101 f. Trabalho de Conclusão de Curso (Tecnólogo em Gestão da Tecnologia da Informação) - Instituto Federal de Educação, Ciência e Tecnologia de Santa Catarina, Florianópolis, 2021. Disponível em: https://repositorio.ifsc.edu.br /handle/123456789/1987. Acesso em: 18 ago. 2024.

TIGRE, P. B. **Gestão da Inovação**: A Economia da Tecnologia no Brasil. Rio de Janeiro: Elsevier, 2006.

Zabbix SIA. **Manual do Zabbix - Documentation.** 2024a. Disponível em: https://www.zabbix.com/documentation/6.4/pt/manual. Acesso em: 1 jun. 2024.

_____. **GLPi**. 2024b. Disponível em: https://www.zabbix.com/br/integrations /glpi#glpi. Acesso em: 23 ago. 2024.