Universidade Federal de Ouro Preto
Escola de Minas
CECAU - Colegiado do Curso de
Engenharia de Controle e Automação

Júlia Miranda Valente

MONITORAMENTO DE ATIVOS EM UMA REDE DE COMPUTADORES DE AUTOMAÇÃO COM APLICAÇÃO DA FERRAMENTA ZABBIX

Monografia de Graduação em Engenharia de Controle e Automação

Ouro Preto, 2023

Júlia Miranda Valente

MONITORAMENTO DE ATIVOS EM UMA REDE DE COMPUTADORES DE AUTOMAÇÃO COM APLICAÇÃO DA FERRAMENTA ZABBIX

Trabalho apresentado ao Colegiado do Curso de Engenharia de Controle e Automação da Universidade Federal de Ouro Preto como parte dos requisitos para a obtenção do Grau de Engenheiro(a) de Controle e Automação.

Universidade Federal de Ouro Preto

Orientador: Profa. Adrielle de Carvalho Santana, DSc

Coorientador: Alan Diego Moreira

Ouro Preto

2023

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DE OURO PRETO
REITORIA
ESCOLA DE MINAS
DEPARTAMENTO DE ENGENHARIA CONTROLE E AUTOMACAO

FOLHA DE APROVAÇÃO

Júlia Miranda Valente

Monitoramento de Ativos em uma Rede de Computadores de Automação com Aplicação da Ferramenta Zabbix

Monografia apresentada ao Curso de Engenharia de Controle e Automação da Universidade Federal de Ouro Preto como requisito parcial para obtenção do título de bacharel em Engenharia de Controle e Automação

Aprovada em 25 de agosto de 2023

Membros da banca

Dra. Adrielle de Carvalho Santana - Orientadora (DECAT - Universidade Federal de Ouro Preto)

Alan Diego Moreira - Coorientador (Samarco Mineração)

Dr. Danny Augusto Vieira Tonidandel - Examinador (DECAT - Universidade Federal de Ouro Preto)

Dr. Agnaldo Jose da Rocha Reis - Examinador (DECAT - Universidade Federal de Ouro Preto)

Adrielle de Carvalho Santana, orientadora do trabalho, aprovou a versão final e autorizou seu depósito na Biblioteca Digital de Trabalhos de Conclusão de Curso da UFOP em 28/08/2023

Documento assinado eletronicamente por **Adrielle de Carvalho Santana**, **PROFESSOR DE MAGISTERIO SUPERIOR**, em 28/08/2023, às 12:06, conforme horário oficial de Brasília, com fundamento no art. 6°, § 1°, do Decreto n° 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site http://sei.ufop.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 , informando o código verificador **0578066** e o código CRC **AE5CE86A**.

R. Diogo de Vasconcelos, 122, - Bairro Pilar Ouro Preto/MG, CEP 35402-163
Telefone: 3135591533 - www.ufop.br

Agradecimentos

Neste momento de transição na minha vida, sou profundamente grata por reconhecer que alcançar esta etapa não foi uma jornada solitária. Quero expressar minha gratidão a cada pessoa especial que fez parte dessa trajetória, contribuindo para que eu chegasse até aqui com o melhor resultado possível.

Em primeiro lugar, agradeço a Deus por me guiar em cada passo desta caminhada e me conceder força e perseverança diária. Aos meus amados pais, Tânia e Roberto, meu agradecimento é imenso pelo apoio incondicional, paciência, dedicação, fé e amor. Sou quem sou, graças a vocês! Quero estender meu agradecimento à minha irmã Paula, cuja lealdade, paciência e afeto tornaram essa jornada ainda mais significativa. Vocês são meu pilar e meu porto seguro. Amo vocês infinitamente!

Ao meu amor, Júnior, não há palavras suficientes para expressar o quanto sou grata por ter alguém tão especial ao meu lado. Seu apoio incondicional e a maneira como você compartilha meus sonhos como se fossem seus próprios, são inestimáveis. Você é minha paz e minha fonte de inspiração.

À minha família Miranda Valente, meu profundo agradecimento por terem sido exemplos de ensinamentos, companheirismo, carinho e incentivo ao longo da minha jornada. Suas presenças foram fundamentais em minha vida.

Aos meus amigos da graduação, em especial a Priscila, as Larissas, o Matheus, o Richard e o Israel, agradeço de coração por todos os momentos compartilhados. Sem a parceria de vocês, essa caminhada teria sido muito mais árdua. Vocês tornaram cada obstáculo mais leve e cada vitória mais significativa.

À equipe de automação da Samarco, especialmente Alan, Alexandre e Lucas, sou imensamente grata pelos ensinamentos valiosos e pela confiança depositada em mim. Vocês fizeram e fazem a diferença em minha jornada acadêmica e profissional, e contribuíram para o desenvolvimento deste trabalho.

Quero expressar minha gratidão à professora Dr^{a}. Adrielle por sua orientação, ensinamentos e apoio ao longo da graduação e da elaboração desta monografia. Aos professores dos departamentos de Engenharia de Controle e Automação, o meu muito obrigada.

Aos demais que cruzaram o meu caminho e contribuíram para este momento, o meu muito obrigada! Serei eternamente grata a todos vocês por essa conquista. Que possamos continuar trilhando caminhos de sucesso e felicidade juntos. Obrigada por fazerem parte da minha vida!

Conheça todas as teorias,
domine todas as técnicas, mas
ao tocar uma alma humana, seja
apenas outra alma humana.

— Carl Gustav Jung.

Resumo

Em uma mina com uma ampla arquitetura de rede, a identificação de problemas representa um desafio significativo. A vasta extensão territorial dificulta a detecção ágil de problemas, levando a consideráveis demoras no tempo de resposta. Especificamente para falhas em ativos como switches, rádios e controladores lógicos programáveis (CLPs), o impacto é evidente. Nessas ocorrências, a realização de medidas corretivas é excessivamente prolongada, resultando em potenciais atrasos no processo produtivo. A carência de um sistema de monitoramento proativo e em tempo real, intensifica essa situação e prejudica a adoção de uma abordagem preditiva. O monitoramento contínuo e em tempo real dos ativos desempenha um papel crucial ao antecipar e resolver problemas antes que adquiram proporções críticas. Além de acelerar a resposta, essa abordagem preventiva impede que problemas iniciais se desenvolvam em questões prejudiciais à eficiência das operações e, ainda mais crucial, à segurança operacional e à infraestrutura de rede. Este estudo de caso tem como foco avaliar a contribuição do monitoramento de ativos, por meio da ferramenta *open source* Zabbix, para aprimorar a eficiência e segurança operacional em um contexto de mineração. Os objetivos abrangem a exploração do Zabbix, sua contribuição para a cibersegurança, sua eficácia no diagnóstico e prevenção de falhas, o entendimento e teste de seus recursos, além de mapear a arquitetura de rede vigente do ambiente a ser monitorado. O estudo incluiu uma revisão sobre alguns conceitos de redes de computadores e sobre o Zabbix, expandindo o entendimento de suas funcionalidades. A implementação da ferramenta permitiu o monitoramento contínuo de ativos em rede de automação e os resultados comprovaram sua eficácia em reforçar a segurança da rede, aprimorar a detecção de falhas e viabilizar manutenções preditivas, contribuindo para orientar futuros trabalhos.

Palavras-chaves: tecnologia, automação, redes de computadores, ativos, manutenção preditiva, monitoramento, cibersegurança e Zabbix.

Abstract

In a mine with a large network architecture, troubleshooting poses a significant challenge. The vast territorial extension makes it difficult to quickly detect problems, leading to considerable delays in the response time. Specifically for failures in assets such as switches, radios and programmable logic controllers (PLCs), the impact is evident. In these occurrences, carrying out corrective measures takes time, resulting in potential delays in the production process. The lack of a proactive and real-time monitoring system intensifies this situation and hinders the adoption of a predictive approach. Continuous, real-time monitoring of assets plays a crucial role in anticipating and resolving issues before they reach critical proportions. In addition to speeding response, this preemptive approach prevents teething problems from developing into issues around the efficiency of operations and, even more crucially, operational security and network infrastructure. This case study focuses on evaluating the contribution of asset monitoring, through the open source tool Zabbix, to improve operational efficiency and safety in a mining context. The objectives include exploring Zabbix, its contribution to cybersecurity, its effectiveness in diagnosing and preventing failures, understanding and testing its resources, in addition to mapping the current network architecture of the environment to be monitored. The study included a review of some concepts of computer networks and Zabbix, expanding the understanding of its functionalities. The implementation of the tool helped the continuous monitoring of automation network assets and the results proved its effectiveness in strengthening network security, improving fault detection and enabling predictive maintenance, helping to guide future work.

Key-words: technology, automation, computer network, active, predictive maintenance, monitoring, cybersecurity and Zabbix.

Lista de ilustrações

Figura 1 – Cartão Perfurado 19
Figura 2 – Mapa Lógico da Rede ARPANET em 1974 20
Figura 3 – Quotas de Mercado de Redes Industriais em 2023 23
Figura 4 – Topologia em Estrela - Com 4 dispositivos 24
Figura 5 – Topologia em Barramento - Com 3 dispositivos 24
Figura 6 – Topologia em Anel - Com 6 dispositivos 25
Figura 7 – Topologia em Malha - Com 5 dispositivos e 10 conexões 25
Figura 8 – Tipos de Redes de Computadores: LAN, WAN, MAN 26
Figura 9 – Camadas da Arquitetura TCP/IP 28
Figura 10 – Ativos em Redes Industriais 29
Figura 11 – Sistema SNMP 30
Figura 12 – Arquitetura do Zabbix 36
Figura 13 – Resumo de Informações da VM 40
Figura 14 – Tela de Login do Zabbix 41
Figura 15 – Dashboard criado no Zabbix 42
Figura 16 – Formulário para Criar um Host 43
Figura 17 – Associação de Templates ao Host 43
Figura 18 – Alguns Hosts com os Templates Associados 44
Figura 19 – Formulário para Criar um Host Group 44
Figura 20 – Host Groups 45
Figura 21 – Formulário para Criar um Mapa no Zabbix 46
Figura 22 – Formulário para Configurar um Elemento no Mapa 46
Figura 23 – Mapas Criados 47
Figura 24 – Criando um Usuário 48
Figura 25 – Mapeamento da Arquitetura de Rede da Mina 49
Figura 26 – Controle das Portas de um Switch 49
Figura 27 – Monitoramento da Rede da Mina: Anteriormente 50
Figura 28 – Monitoramento da Rede da Mina: Atualmente 51
Figura 29 – Monitoramento de Throughput 52
Figura 30 – Monitoramento da Temperatura de um Switch 52
Figura 31 – Monitoramento do Tráfico de Rede de um Switch 53
Figura 32 – Relatório de Disponibilidade: ICMP Ping 53
Figura 33 – Action Log: Problema de Temperatura 54
Figura 34 – Dados mais Recentes de um Switch 54
Figura 35 – Monitoramento do Mineroduto 55
Figura 36 – Monitoramento do Backbone 55

Lista de abreviaturas e siglas

ANSI	American National Standards Institute - Instituto Norte Americano de Padrões
API	Application Programming Interface - Interface de Programação de Aplicação
ARPA	Advanced Research Projects Agency - Agência de Projetos de Pesquisa Avançada
ARPANET	Advanced Research Projects Agency Network - Rede da Agência de Pesquisas em Projetos Avançados
CERN	European Organization for Nuclear Research - Organização Europeia para a Pesquisa Nuclear
CPU	Central Processing Unit - Unidade Central de Processamento
DNS	Domain Name System - Sistema de Nome de Domínio
DoD	Department of Defense - Departamento de Defesa
Ethernet	Arquitetura de Interconexão para Redes Locais
FTP	File Transfer Protocol - Protocolo de Transferência de Arquivo
GPLv2	GNU General Public License version 2 - Licença Pública Geral GNU versão 2
HTTP	Hypertext Transfer Protocol - Protocolo de Transferência de Dados
ICMP	Internet Control Message Protocol - Protocolo de Controle de Mensagem
IEC	International Electrotechnical Commission - Comissão Eletrotécnica Internacional
IEEE	Institute of Electrical and Electronics Engineers - Instituto de Engenheiros Eletricistas e Eletrônicos
IHM	Human Machine Interface - Interface Homem-Máquina
IIoT	Industrial Internet of Things - Internet Industrial das Coisas
IoT	Internet of Things - Internet das Coisas

IP	Internet Protocol - Protocolo de Internet
IPMI	Intelligent Platform Management Interface - Interface Inteligente de Gerenciamento de Plataforma
LAN	Local Area Network - Rede de Área Local
M2M	Machine to Machine - Máquina para Máquina
MAN	Metropolitan Area Network - Rede de Área Metropolitana
MIB	Management Information Base - Base de Informações de Gerenciamento
OID	Object Identifier - Identificador de Objeto
PdM	Predictive Maintenance - Manutenção Preditiva
PLC	Programmable Logic Controller - Controlador Lógico Programável
SCADA	Supervisory Control And Data Acquisition - Sistema de Supervisão e Aquisição de Dados
SGBD	Data Base Management System - Sistema de Gerenciamento de Banco de Dados
SLA	Service Level Agreement - Acordo de Nível de Serviço
SMTP	Simple Mail Transfer Protocol - Protocolo Transferência de Mensagem Simples
SNMP	Simple Network Management Protocol - Protocolo de Gerenciamento Simples de Rede
SSH	Secure Shell - Protocolo de Segurança de Troca de Arquivos Entre Cliente e Servidor
SSL	Secure Socket Layer - Camada de Soquete Seguro
TA	Automation Technology - Tecnologia da Automação
TCP	Transmission Control Protocol - Protocolo de Controle de Transmissão
TCP/IP	Transmission Control Protocol/Internet Protocol - Protocolo de Transmissão e Controle/Protocolo de Internet
Telnet	Protocolo de Internet Para Acesso Virtual via Terminal Virtual
TI	Information Technology - Tecnologia da Informação

TLS	Transport Layer Security - Segurança da Camada de Transporte
TO	Operational Technology - Tecnologia Operacional
WWW	World Wide Web - Rede de Alcance Mundial
UDP	User Datagram Protocol - Protocolo de Datagrama de Usuário
WAN	Wide Area Network - Rede de Longa Distância
WLAN	Wireless Local Area Network - Rede de Área Local Sem Fio

Sumário

1 INTRODUÇÃO . . . 13
1.1 Justificativas e Relevância . . . 14
1.2 Objetivos . . . 15
1.2.1 Objetivo Geral . . . 15
1.2.2 Objetivos Específicos . . . 15
1.3 Metodologia . . . 15
1.4 Organização e estrutura . . . 15

2 REVISÃO DE LITERATURA . . . 17
2.1 Tecnologia da Informação . . . 17
2.2 Tecnologia Operacional . . . 18
2.3 Convergência entre TI e TO . . . 18
2.4 Uma Breve História das Redes de Computadores . . . 19
2.5 Redes de Computadores . . . 21
2.5.1 Redes Industriais . . . 22
2.5.2 Topologias de Rede . . . 23
2.5.3 Principais Tipos de Redes . . . 25
2.5.4 Modelo de Referência TCP/IP . . . 27
2.5.5 Ativos em uma Rede Industrial . . . 28
2.5.6 Protocolo SNMP . . . 29
2.5.7 Protocolo SSH . . . 30
2.6 Cibersegurança . . . 31
2.7 Gerenciamento de Redes . . . 32
2.7.1 Monitoramento . . . 32
2.7.2 Controle . . . 33
2.8 Manutenção Preditiva . . . 33

3 FERRAMENTA DE MONITORAMENTO ZABBIX . . . 35
3.1 Arquitetura . . . 35
3.2 Definições . . . 37
3.3 Segurança . . . 38

4 PROJETO PROPOSTO . . . 39
4.1 Apresentação do Ambiente . . . 39
4.2 Delimitação do Monitoramento . . . 39
4.3 Instalação e Configuração . . . 40

4.3.1 *Hosts* 42
4.3.2 *Host Groups* 44
4.3.3 *Maps* 45
4.3.4 *Users* 47
4.4 Monitoramento *Web* **48**

5 CONCLUSÃO **56**

Referências **57**

1 Introdução

A Indústria 4.0 traz termos para o setor industrial que há alguns anos não eram conhecidos, como inteligência artificial, internet das coisas, robótica, integração de sistemas, nuvem e cibersegurança. Porém, atualmente, essas tecnologias já fazem parte do cotidiano de todas as empresas.

Esse desenvolvimento tecnológico em grande escala, conhecido também como a 4ª Revolução Industrial, está mudando de forma expressiva a automação, as etapas de produção e as redes de controle e comunicação por meio do uso de tecnologias, ferramentas e técnicas que garantam a inovação, a agilidade, eficiência e customização dos processos produtivos industriais e dos sistemas de gestão.

As redes de computadores são fundamentais para o bom funcionamento e alto desempenho de uma organização. Com a exigência crescente de uma indústria altamente conectada, a integração entre os sistemas de Tecnologia da Informação (TI) e Operacional (TO) vem se tornando cada vez mais inevitável. A busca constante por ferramentas *open source*, tecnologias de ponta e de baixo custo, faz com que os sistemas de TI e TO busquem por soluções em conjunto, seguindo cada vez mais interligados.

Essa integração entre sistemas de TO e TI, em conjunto com a crescente necessidade por troca de dados e informações entre ambos, tornam as redes de computadores um ponto delicado dentro das empresas e suas respectivas plantas industriais. Vale lembrar que empresas competitivas, não toleram paradas, problemas de desempenho, falta de diagnósticos e indisponibilidade das redes. Esses problemas comprometem o processo produtivo e como consequência geram prejuízos e impactos negativos nos resultados das organizações.

Além disso, essa crescente integração com os sistemas de TI, faz com que a vulnerabilidade seja um risco dessa modalidade para os sistemas de TO, no que se diz respeito aos aspectos de segurança contra acessos indevidos, roubos de informações e ataques de *hackers*.

O ato de gerenciar e monitorar os ativos presentes em uma rede tende a trazer muitos benefícios para a infraestrutura e os sistemas produtivos, garantindo um sistema robusto, eficaz e seguro o suficiente para que se consiga melhores resultados.

O monitoramento de redes é o controle de qualquer ativo capaz de ser monitorado em uma estrutura de rede e que podem ser distribuídos em diversos locais em uma planta, sejam eles próximos ou não.

O monitoramento de ativos em uma rede é um processo responsável por verificar em

tempo real, 24 horas por dia, 7 dias por semana, o funcionamento desses ativos e o estado da sua conexão na rede, ou seja, é responsável por detectar anomalias de desempenho e disponibilidade, de forma que seja possível ter uma atuação preditiva.

Utilizar ferramentas de gerenciamento e monitoramento de redes pode ser muito útil para manter os processos produtivos de uma organização em segurança, além de permitir uma atuação preditiva frente a possíveis falhas e paradas das atividades.

O Zabbix é uma dessas ferramentas, com ele é possível monitorar vários componentes em uma rede, bem como a disponibilidade dos ativos e serviços.

O *software* de monitoramento de redes Zabbix, é *open source*, bastante utilizado para o monitoramento de dispositivos em uma rede, possui uma *interface* 100% *web* e suporta o Protocolo Simples de Gerenciamento de Redes/*Simple Network Managent Protocol* (SNMP). Além disso, conta com alertas de eventos altamente confiáveis, gráficos e *dashboards* personalizados, histórico e *syslog* de eventos, além de armazenamento de dados, monitoramento de *throughput* (taxa de transferência), monitoramento de temperatura dos ativos e monitoramento de *interfaces*.

1.1 Justificativas e Relevância

Em uma planta industrial, principalmente em áreas de grande extensão territorial, como, por exemplo, uma mina de extração de minério de ferro, é comum uma indisponibilidade de equipamentos ser identificada somente depois de um longo período após a ocorrência da falha, gerando um aumento no tempo de resposta e, em alguns casos, ocasionando a parada do processo produtivo. Para uma infraestrutura de rede adequada, eficaz, segura e aderente, é necessário um monitoramento de ativos que garanta uma estabilidade e segurança na gestão, no controle e na operação dos processos.

Ao optar por utilizar uma ferramenta que monitore a planta industrial é possível melhorar a disponibilidade da rede, tornando mais simples a detecção de possíveis problemas com antecedência. Dessa forma é possível atuar de forma preditiva, minimizando os impactos nos processos. Assim pode-se diminuir, de forma significativa, problemas como: perda de comunicação entre ativos, perda de comunicação entre os sistemas supervisórios e os ativos em campo, problemas relacionados à saúde dos ativos (como roteadores, *switch*, servidores, clps, entre outros). A implementação de um *software* de gerenciamento e monitoramento de rede oferece um maior controle e atuação sobre o ambiente industrial, maior agilidade na identificação e diagnóstico de falhas, aumento na produtividade, redução dos riscos e redução de custos para a empresa. Assim, justifica-se a realização deste trabalho para que se possa observar, na prática, os benefícios da implementação de tal *software*.

1.2 Objetivos

1.2.1 Objetivo Geral

O objetivo deste trabalho consiste em realizar um estudo de caso, mostrando como o monitoramento de ativos em uma infraestrutura de rede de computadores, utilizando a ferramenta *web* gratuita e de código aberto Zabbix, pode contribuir com a cibersegurança, além de proporcionar um maior controle na identificação de falhas em uma empresa de mineração.

1.2.2 Objetivos Específicos

- Ampliar o conhecimento do *software* Zabbix.
- Analisar como o Zabbix pode contribuir com a cibersegurança.
- Conhecer e testar alguns dos recursos ofertados pelo Zabbix.
- Implementar o Zabbix para monitorar os ativos em rede de automação em uma empresa do ramo da mineração.
- Analisar o comportamento do Zabbix no diagnóstico e prevenção de falhas.

1.3 Metodologia

Este trabalho tem como finalidade a realização de um estudo de caso com o intuito de compreender e analisar o uso da ferramenta Zabbix para o monitoramento de ativos em uma rede de computadores. A classificação desta pesquisa quanto aos seus objetivos, se divide em exploratória e descritiva. O estudo conta com a abordagem qualitativa e tem como foco um estudo de caso sobre a relação do Zabbix com a cibersegurança, e a possibilidade do seu uso oferecer um maior controle na identificação de falhas em uma empresa do ramo da mineração.

Para a execução desse trabalho é adotado o método de pesquisa bibliográfica, com a realização de análises de artigos acadêmicos, trabalhos de conclusão de curso e literaturas especializadas. Além disso, é realizado um estudo de caso sobre a implementação da ferramenta Zabbix em uma empresa do setor de mineração com o intuito de facilitar o entendimento, a análise e a realização dos objetivos deste trabalho.

1.4 Organização e estrutura

Este trabalho está organizado da seguinte forma:

No Capítulo 1 é feita uma breve introdução ao tema que será abordado durante todo o trabalho e os objetivos desse. No Capítulo 2 é feita uma fundamentação teórica dos pontos principais utilizados como embasamento teórico para a realização do presente trabalho. São abordados conceitos sobre tecnologia da informação e tecnologia operacional, redes de computadores, cibersegurança, gerenciamento de redes e manutenção preditiva, além de outros pontos relacionados a esses tópicos. No Capítulo 3 são apresentados conceitos referentes a ferramenta Zabbix e seu funcionamento. No Capítulo 4 é apresentado o estudo de caso, sendo detalhado o ambiente proposto, bem como a configuração dos recursos do Zabbix e o monitoramento em tempo real do ambiente. No Capítulo 5, são feitas as considerações finais do trabalho, bem como as sugestões para trabalhos futuros.

2 Revisão de literatura

Neste segmento, serão expostos os conceitos fundamentais e as tecnologias essenciais que estão ligadas à automação e à supervisão de redes usando o Zabbix. Essa exposição serve como uma base para compreender a necessidade de uso da ferramenta de monitoramento e o modo como ela opera no cenário proposto.

2.1 Tecnologia da Informação

Segundo Laudon e Laudon (2016), a Tecnologia da Informação (TI) é uma área que engloba diversas disciplinas e envolve o uso de computadores, redes, sistemas e *softwares* para capturar, processar, armazenar, transmitir e administrar informações de maneira eficaz. Em resumo, a TI se concentra na aplicação de tecnologia para tratar dados e informações em vários setores, incluindo negócios, ciência, educação, saúde, entretenimento e outras áreas.

Com base em Turban, Volonino e Wood (2015) a TI é responsável por envolver diferentes áreas, como:

- Coleta, processamento, armazenamento e análise de dados: possibilitando a obtenção de dados brutos por meio de diversos meios, após a coleta, os dados são armazenados e submetidos a processos de transformação e análise para extrair *insights* e padrões importantes.
- Transmissão e Comunicação: transmitindo as informações por meio de redes de comunicação, como a internet, possibilitando assim, a conexão global.
- Automatização: sendo amplamente empregada para automatizar tarefas e processos, aumentando a eficiência e a produtividade.
- Desenvolvimento de Software: A criação de *software* personalizado é uma parte essencial da tecnologia da informação, atendendo às necessidades específicas de indivíduos e organizações.
- Segurança da Informação: implementando medidas e estratégias para proteger dados e sistemas contra ameaças cibernéticas, garantindo a confidencialidade, integridade e disponibilidade das informações.

A TI é um campo em constante evolução, impulsionando o desenvolvimento de novas tecnologias, como inteligência artificial, Internet das Coisas (IoT) e realidade virtual.

Dessa forma, ela impulsiona a evolução da sociedade do conhecimento e transforma a maneira como vivemos, trabalhamos e nos conectamos (CARTER, 2013).

2.2 Tecnologia Operacional

A Tecnologia Operacional (TO) é um conjunto de recursos, dispositivos e *softwares* projetados para monitorar, controlar e aprimorar os procedimentos industriais de maneira específica. Diferentemente da tecnologia da informação, que se concentra em dados e questões administrativas, a TO está voltada para os aspectos físicos e operacionais das indústrias, com o objetivo de aperfeiçoar a eficiência, segurança e excelência dos produtos ou serviços fornecidos (HAUG; HINTERHUBER, 2017).

A TO abrange diversas tecnologias e conceitos, como automação industrial, controle de processos, instrumentação, sensoriamento, sistemas de supervisão e aquisição de dados (SCADA), Internet das Coisas Industrial (IIoT), cibersegurança, entre outros (LEE; BAGHERI; KAO, 2015).

2.3 Convergência entre TI e TO

Segundo Lee, Bagheri e Kao (2015), a convergência entre tecnologia da informação e tecnologia operacional envolve a integração e cooperação dessas duas áreas tecnológicas diferentes com o propósito de melhorar e otimizar os processos industriais e operacionais. Esse alinhamento estratégico é motivado pelo crescente processo de digitalização e automação nas indústrias, que demanda uma combinação eficiente dos recursos de TI com os sistemas de TO para alcançar uma maior eficiência e eficácia nas operações e processos.

Anteriormente, os sistemas de TO operavam de forma isolada, porém, agora estão sendo mais frequentemente integrados a redes, o que resulta na geração e utilização de grandes volumes de dados. Além disso, *softwares* que costumavam ser exclusivamente utilizados pelas equipes de TI, passaram a ser empregados para dar suporte aos processos de TO (IBE, 2001).

Essa integração entre TO e TI se estende além disso. Muitos setores estão adotando plataformas tecnológicas que permitem unificar os dados dispersos que antes eram usados separadamente para fins empresariais e operacionais. Esse cenário é uma mudança significativa para os processos industriais, que costumavam operar de forma isolada, sem se conectar a outros sistemas (PEDRIALI, 2021).

Para Haug e Hinterhuber (2017), a convergência da tecnologia operacional com outras tecnologias emergentes, como a TI, a IIoT e a *Machine to Machine* (M2M), tem impulsionado ainda mais o avanço da indústria em direção à Indústria 4.0.

O resultado da convergência é a criação de um sistema unificado, o que, por sua vez, oferece novas oportunidades para as empresas utilizarem esses dados de forma mais eficiente. A possibilidade de unificar os dados de TO e TI proporciona uma visão mais ampla e completa dos processos de negócio, permitindo às empresas tomarem decisões mais embasadas e eficientes, possibilitando uma abordagem abrangente dos processos industriais, com o objetivo de melhorar a sua produtividade e desempenho em geral (PEDRIALI; GALEGALE; ARIMA, 2022).

Com base em Sengupta, Ruj e Das Bit (2020), apesar dos benefícios, essa integração com a TI, expõe a TO a ameaças cibernéticas mais sofisticadas, resultando em riscos graves como violações de dados, sabotagem de processos industrais e até mesmo, interrupção completa das operações. Em ambientes industriais, a disponibilidade e integridade dos sistemas são cruciais. Portanto, investir em medidas de segurança, como *firewalls*, criptografia, treinamentos e monitoramento de rede, são algumas das estratégias que podem ser adotadas para mitigar os riscos de segurança decorrentes da convergência entre TI e TO.

2.4 Uma Breve História das Redes de Computadores

Segundo Monqueiro (2008), as redes de computadores passaram por um extenso processo de desenvolvimento antes de atingirem os padrões comuns utilizados hoje em dia. Durante a década de 60, surgiram as primeiras redes de computadores como uma maneira de possibilitar a transferência de informações entre diferentes computadores. Nessa época, os cartões perfurados ainda eram o meio mais utilizado para o armazenamento externo de dados e o transporte, sendo capazes de armazenar apenas algumas dezenas de caracteres cada. A Figura 1 ilustra um cartão perfurado.

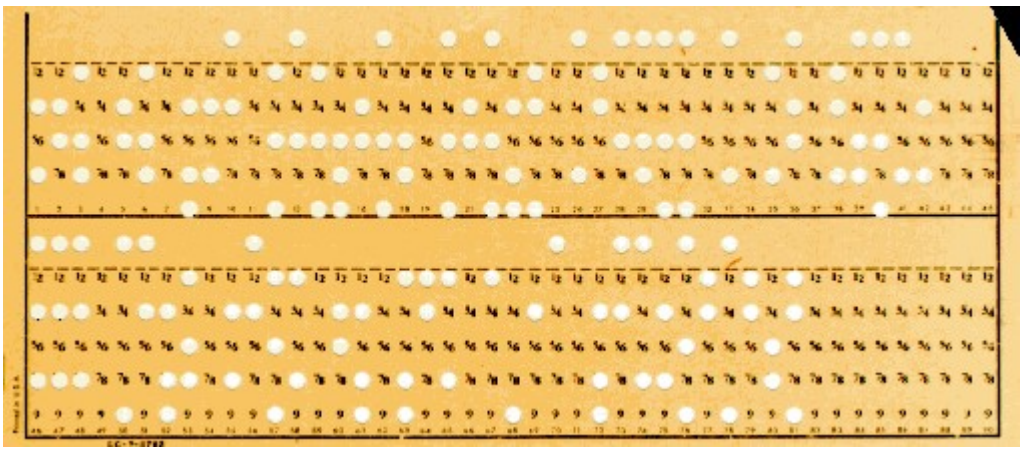


Figura 1 – Cartão Perfurado

Fonte: Monqueiro (2008)

Em 1966, a ARPANET foi criada com a liderança de Lawrence Roberts, e tinha como objetivo interconectar computadores de pesquisa financiados pela ARPA. Em 1969, a ARPANET tornou-se operacional, conectando os primeiros quatro nós da rede: Universidade da Califórnia em Los Angeles, Instituto de Pesquisa de Stanford, Universidade da Califórnia em Santa Bárbara e Universidade de Utah. A ARPANET é considerada um marco histórico para o desenvolvimento das redes de computadores e para o surgimento da internet (HAFNER; LYON, 1998).

Inicialmente, a Arpanet tinha como propósito conectar apenas quatro computadores com diferentes arquiteturas para testar a troca de dados entre eles. No entanto, a rede se expandiu rapidamente, e até 1973, já estava conectando 30 instituições, incluindo universidades, instituições militares e empresas, a Figura 2 ilustra a rede da Arpanet em 1974. Os responsáveis pelo projeto tinham uma preocupação central em garantir uma operação eficiente, buscando alcançar a maior disponibilidade possível de conexão (MONQUEIRO, 2008).

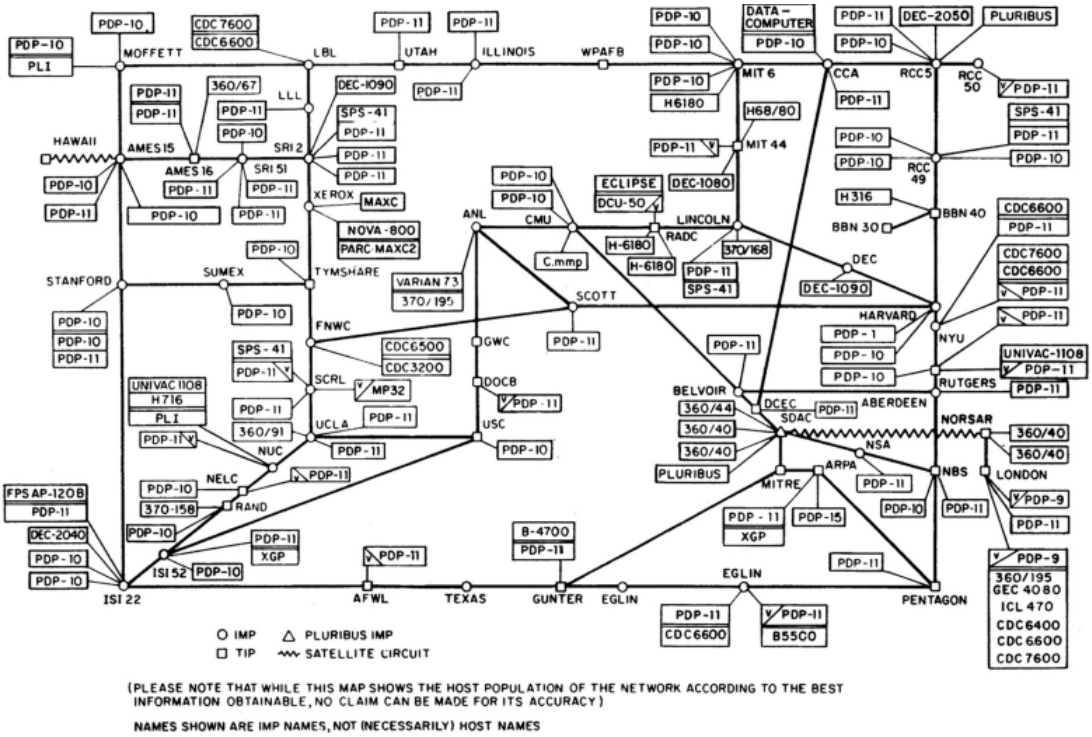


Figura 2 – Mapa Lógico da Rede ARPANET em 1974

Fonte: Fidler e Currie (2015)

Na década de 1974, foi introduzido o TCP/IP, um protocolo que se tornou essencial para a ARPANET e, posteriormente, para a internet. Por meio de uma rede conectando várias universidades, o TCP/IP possibilitou o fluxo livre de informações, o que impulsionou o desenvolvimento de recursos fundamentais ainda em uso atualmente. Entre esses recursos

estão o e-mail, o telnet e o FTP, que permitiram aos usuários conectados a troca de informações, acesso a computadores remotos e compartilhamento de arquivos (ALENCAR, 2010).

O rápido crescimento da rede trouxe um desafio: identificar os computadores de forma eficiente. O uso de números IP como rótulos tornou-se difícil à medida que mais computadores foram adicionados, para resolver esse problema, em novembro do mesmo ano, os pesquisadores Jon Postel, Paul Mockapetris e Craig Partridge criaram o serviço DNS *(Domain Name System)*. Esse serviço associava nomes de fácil entendimento a cada endereço IP, simplificando a interação entre pessoas e computadores na rede. Em 1984, o DNS foi implementado na Internet, dando origem aos domínios e no ano seguinte, em 1985, a Internet já contava com dois mil computadores interconectados, marcando o início de sua expansão significativa (MACEDO et al., 2018).

Com o crescente aumento do número de computadores conectados à Internet, ficou claro para muitos pesquisadores a importância de um protocolo que pudesse gerenciar tanto os computadores quanto os serviços oferecidos pelas redes. Para atender a essa demanda, foi criado o protocolo SNMP *(Simple Network Management Protocol)* (MACEDO et al., 2018).

Em 1989, Tim Berners-Lee criou a *World Wide Web* (WWW), durante o período em que estava empregado no CERN (Organização Europeia para a Pesquisa Nuclear). Seu objetivo era estabelecer um sistema que facilitasse a troca de informações entre cientistas de diversas regiões do globo. Para isso, ele introduziu o conceito de hipertexto e hipermídia, tornando a navegação e a busca por informações mais eficazes (BERNERS-LEE, 2000).

Essas inovações foram cruciais para moldar a internet como a conhecemos hoje, gerando um grande impacto positivo e importante para a revolução da internet (MACEDO et al., 2018).

2.5 Redes de Computadores

De acordo com Kurose e Ross (2017), as redes de computadores são sistemas que permitem a conexão e a troca de dados entre dispositivos, como computadores, servidores, roteadores e *switches*. Elas desempenham um papel essencial na comunicação e no compartilhamento de informações em diversos ambientes, abrangendo desde redes locais simples até a vasta rede global conhecida como Internet. As redes de computadores são desenvolvidas utilizando uma ampla gama de tecnologias e protocolos, os quais estabelecem diretrizes e normas para o envio e recebimento de dados (PETERSON; DAVIE, 2012).

Para Tanenbaum e Wetherall (2010), as redes de computadores podem ser definidas como sistemas que permitem a interconexão de dispositivos, possibilitando a comunicação

e o compartilhamento de recursos. Ademais, Tanenbaum e Wetherall (2010) descreve as redes de computadores como sistemas compostos por nós, que representam os dispositivos, e enlaces de comunicação, que correspondem aos meios físicos ou lógicos de transferência de dados entre esses nós. Essa estrutura permite a troca eficiente de informações e recursos entre os dispositivos conectados à rede.

2.5.1 Redes Industriais

Redes industriais são estruturas de comunicação que possibilitam a troca de dados entre dispositivos e equipamentos empregados em contextos industriais. Essas redes desempenham um papel essencial na automação industrial, permitindo que máquinas, sensores, atuadores e sistemas de controle sejam interligados em uma única infraestrutura (LUGLI; SANTOS, 2010).

As redes industriais podem ser classificadas em diferentes tipos, dependendo das características e requisitos específicos de cada aplicação. Alguns dos principais tipos de redes industriais incluem (GALLOWAY; HANCKE, 2012):

- Ethernet Industrial: é uma forma de rede baseada na tecnologia Ethernet padrão, sendo amplamente adotada na indústria devido à sua alta velocidade e confiabilidade. Dentre os protocolos mais comuns tem-se: o PROFINET, o EtherNet/IP e o Modbus TCP.
- Fieldbus: são redes desenvolvidas para substituir as conexões ponto a ponto encontradas em sistemas de controle tradicionais. Essas redes permitem a comunicação serial entre dispositivos no campo, como sensores e atuadores, e o controlador principal. Algumas das redes Fieldbus mais conhecidas são o PROFIBUS, FOUNDATION Fieldbus e DeviceNet.
- Redes industriais sem fio: essas redes oferecem flexibilidade e mobilidade na comunicação, especialmente em ambientes com cabeamento complexo ou de difícil acesso. Como exemplo de redes industriais sem fio, tem-se o WirelessHART.

Anualmente, a HMS Networks realiza uma análise do mercado de redes industriais para avaliar como estão sendo distribuídos os novos dispositivos conectados na automação das fábricas, conforme ilustrado na Figura 3. De acordo com o estudo deste ano, é previsto um crescimento de 7% no mercado de redes industriais em 2023.

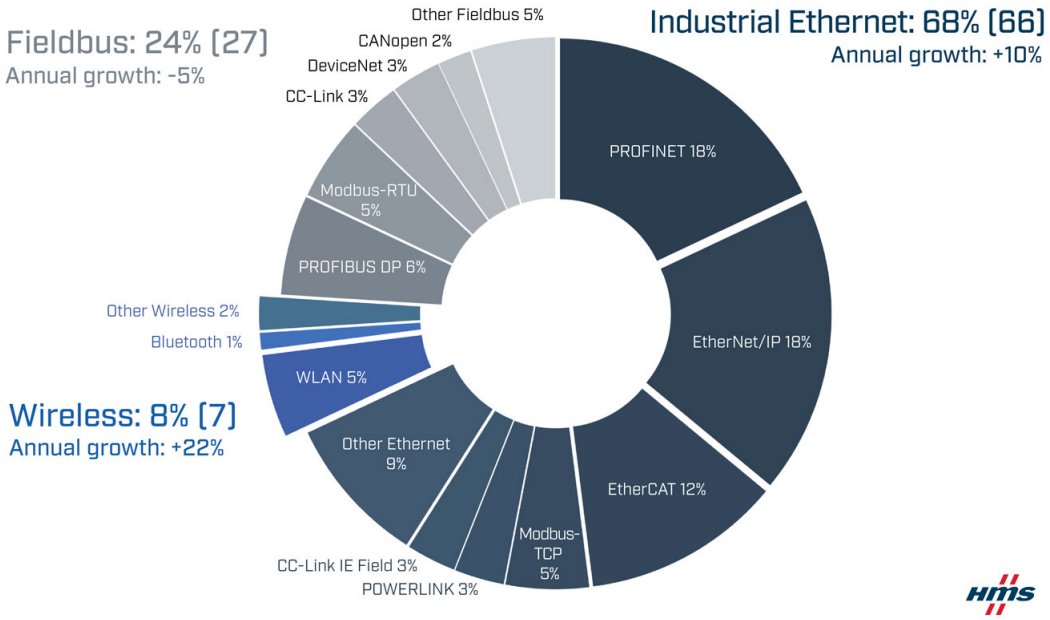


Figura 3 – Quotas de Mercado de Redes Industriais em 2023

Fonte: Carlsson (2023)

2.5.2 Topologias de Rede

Segundo Tonidandel (2010), as topologias de rede dizem respeito à forma como os dispositivos se conectam em uma rede de computadores. Elas estabelecem a organização física e lógica da rede, determinando como os dados são enviados e recebidos entre esses dispositivos. Existem diversas topologias de rede comuns, cada uma com suas próprias características e usos específicos.

De acordo com Forouzan (2013) e Alencar (2010), dentre as principais topologias de rede, pode-se destacar:

- Topologia em Estrela: todos os dispositivos estão ligados a um ponto central, como um *hub* ou *switch*. Esse ponto central atua como um intermediário que controla o fluxo de dados entre os dispositivos conectados. Uma vantagem dessa topologia é que, caso um dispositivo apresente falhas, os outros dispositivos não serão impactados. No entanto, se o ponto central falhar, toda a rede pode ficar inativa, vide Figura 4.

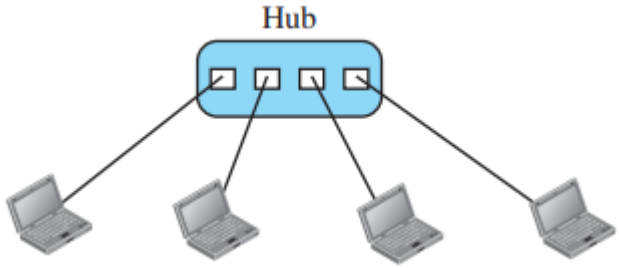


Figura 4 – Topologia em Estrela - Com 4 dispositivos

Fonte: Forouzan (2013)

- Topologia em Barramento: todos os dispositivos são interligados por um único cabo compartilhado, chamado de barramento. Os dados são enviados por esse barramento e recebidos por todos os dispositivos na rede. Apesar de ser simples de configurar, essa topologia pode estar propensa a colisões de dados e, caso o cabo principal tenha problemas, toda a rede será impactada, vide Figura 5.

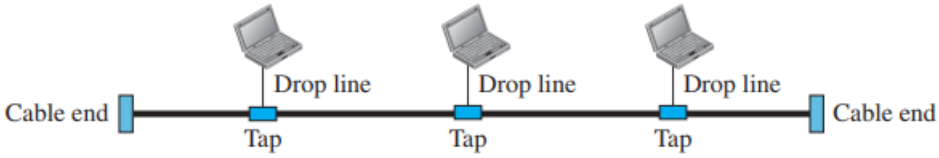


Figura 5 – Topologia em Barramento - Com 3 dispositivos

Fonte: Forouzan (2013)

- Topologia em Anel: os dispositivos são interligados em um anel fechado, onde cada dispositivo está conectado ao dispositivo vizinho mais próximo, criando um circuito contínuo. Os dados circulam ao longo desse anel até chegarem ao destinatário correto. Embora seja uma forma eficiente de transmitir dados, a falha de apenas um dispositivo pode causar a interrupção completa da comunicação em toda a rede, vide Figura 6.

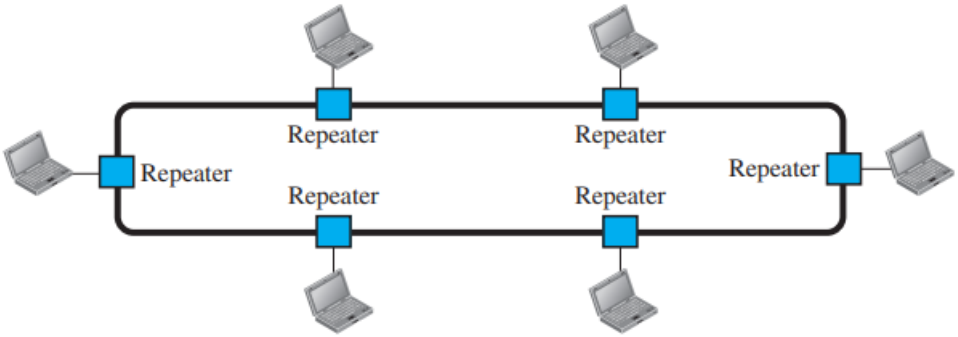


Figura 6 – Topologia em Anel - Com 6 dispositivos

Fonte: Forouzan (2013)

- Topologia em Malha: todos os dispositivos são conectados diretamente uns aos outros, possibilitando várias rotas para a transmissão de dados. A topologia em malha pode ser parcial, onde alguns dispositivos têm conexões específicas entre si, ou completa, onde todos os dispositivos são conectados uns aos outros. Essa topologia é altamente redundante e pode suportar falhas com resistência, garantindo maior confiabilidade na comunicação. No entanto, sua implementação pode ser de alto custo devido ao grande número de conexões necessárias entre os dispositivos, vide Figura 7.

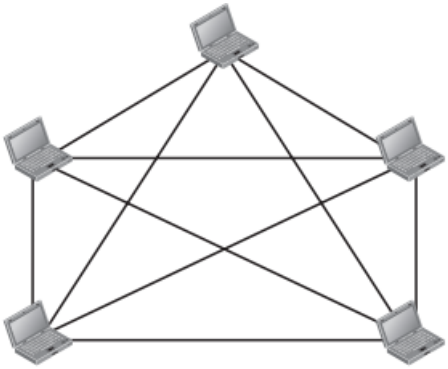


Figura 7 – Topologia em Malha - Com 5 dispositivos e 10 conexões

Fonte: Forouzan (2013)

2.5.3 Principais Tipos de Redes

Existem vários tipos de redes de computadores, cada uma com suas características e propósitos específicos. Para Elias e Lobato (2013), aqui estão alguns dos tipos mais comuns de redes de computadores:

- LAN (*Local Area Network* - Rede de Área Local): uma LAN é uma rede de computadores que se estende por uma área geográfica restrita, como um escritório, uma casa ou um campus universitário. Essas redes locais têm como objetivo facilitar a comunicação e a partilha de recursos entre dispositivos próximos, tais como computadores, impressoras e servidores.

- WLAN (*Wireless Local Area Network* - Rede de Área Local Sem Fio): uma WLAN é uma variante sem fio de uma LAN, onde os dispositivos se conectam à rede utilizando tecnologias *wireless*, como via Wi-Fi e via rádio. Essas redes sem fio oferecem maior mobilidade aos usuários, permitindo que eles se conectem à rede sem a necessidade de cabos físicos.

- WAN (*Wide Area Network* - Rede de Área Ampla): uma WAN é uma rede que se estende por uma vasta área geográfica, geralmente abrangendo múltiplas cidades, estados ou até mesmo países. A Internet é um exemplo amplamente conhecido de uma WAN, interconectando redes em todo o mundo. Essas redes de longa distância possibilitam a comunicação e o compartilhamento de recursos entre locais geograficamente distantes.

- MAN (*Metropolitan Area Network* - Rede de Área Metropolitana): uma MAN é uma rede que abrange uma área mais ampla do que uma LAN, geralmente em uma cidade ou região metropolitana. Ela interconecta várias LANs e possibilita o compartilhamento de recursos e serviços em uma área geográfica mais extensa.

  A Figura 8 ilustra a área de cobertura das redes LAN, WAN e MAN.

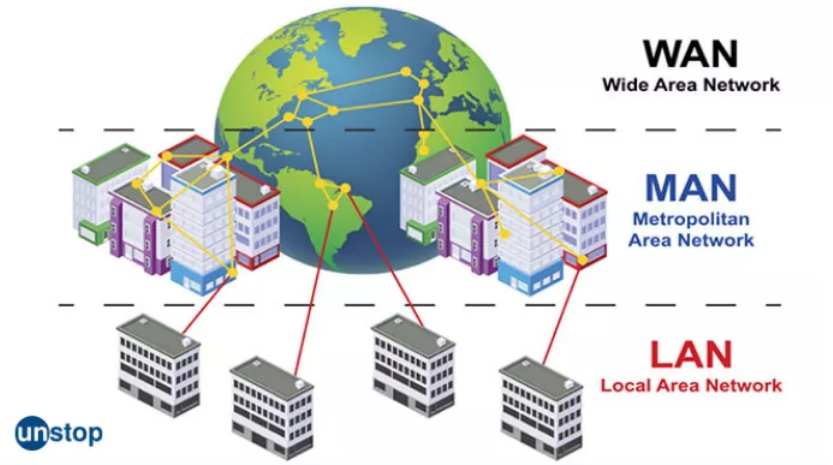


Figura 8 – Tipos de Redes de Computadores: LAN, WAN, MAN

Fonte: Goyal (2022)

2.5.4 Modelo de Referência TCP/IP

O modelo TCP/IP, também conhecido como modelo de protocolo TCP/IP, é um conjunto de padrões de comunicação que forma a infraestrutura fundamental da Internet e de diversas redes de computadores pelo mundo. Surgiu nos anos 1970, conhecido como modelo DoD (*Department of Defense*) e, desde então, se tornou o padrão global para o funcionamento das redes de comunicação (MACEDO et al., 2018).

De acordo com Elias e Lobato (2013), esse modelo organiza o processo de comunicação em diferentes camadas, cada uma com funções específicas e interdependentes. Cada camada presta serviços para a camada acima dela e utiliza os serviços oferecidos pela camada imediatamente abaixo, ilustrado na Figura 9. As principais camadas do modelo TCP/IP são:

- Camada de Aplicação: é a camada mais alta, responsável por gerenciar a interação entre os aplicativos e a rede. É a única camada cuja implementação é realizada através de processos do sistema operacional e trata os detalhes específicos da cada tipo de aplicação. Como exemplo de protocolos que atendem às necessidades dos aplicativos, tem-se: HTTP para páginas da *web*, SMTP para e-mails e FTP para transferência de arquivos.

- Camada de Transporte: encarrega-se de transportar os dados entre os dispositivos finais, garantindo que a entrega ocorra de maneira confiável e organizada. Os principais protocolos nesta camada são o TCP (*Transmission Control Protocol*) e o UDP (*User Datagram Protocol*).

- Camada de Rede: responsável por cuidar do endereçamento e roteamento dos pacotes de dados através da rede. O protocolo mais conhecido nessa camada é o IP (*Internet Protocol*), responsável por atribuir endereços IP aos dispositivos e direcionar o tráfego de dados.

- Camada de Enlace de Dados: também conhecida como camada de *interface* de rede, é responsável por aceitar datagramas IP da camada de rede e transmiti-los, na rede física específica, na forma de quadros. Ela compatibiliza a tecnologia da rede física com o protocolo IP. Geralmente, esta camada inclui o *driver* de dispositivo no sistema operacional e a respectiva placa de rede, tratando os detalhes de *hardware* para conexão física com a rede e transmissão de dados no meio físico. Assim, pode-se dizer que a camada de *interface* de rede é basicamente suportada pela própria tecnologia da rede física.

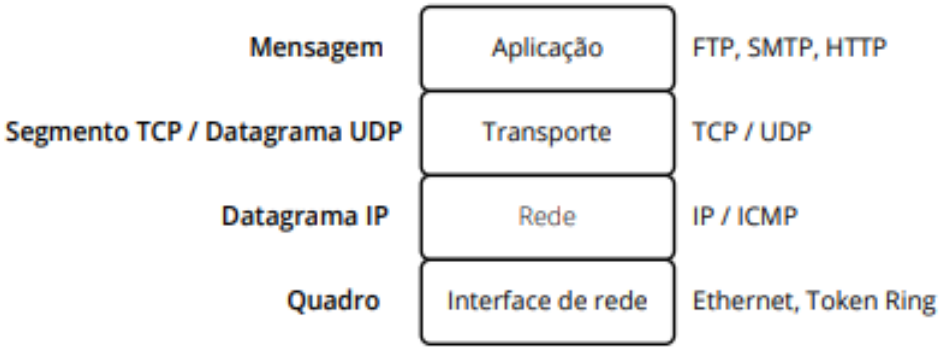


Figura 9 – Camadas da Arquitetura TCP/IP

Fonte: Elias e Lobato (2013)

As vantagens do modelo TCP/IP incluem sua flexibilidade, escalabilidade e capacidade de suportar redes com diferentes tecnologias. Devido a essas características, o modelo TCP/IP se tornou o protocolo predominante para a comunicação de dados em redes de computadores, sendo a base essencial para o funcionamento da Internet moderna.

2.5.5 Ativos em uma Rede Industrial

De acordo com Marshall e Rinaldi (2004), nas redes de computadores industriais, os ativos têm um papel crucial ao interconectar e permitir a comunicação entre os dispositivos utilizados em ambientes de fabricação e produção. Esses ativos são especialmente projetados para atender às exigências específicas da indústria e garantir alta confiabilidade e desempenho em ambientes desafiadores. Alguns dos principais ativos presentes em redes de computadores industriais incluem:

- PLCs (Controladores Lógicos Programáveis), IHMs (*Interface* Homem-Máquina), *switches*, roteadores, *gateways*, rádios, servidores, *firewalls*, entre outros.

A Figura 10 ilustra uma arquitetura de rede industrial e os seus respectivos ativos.

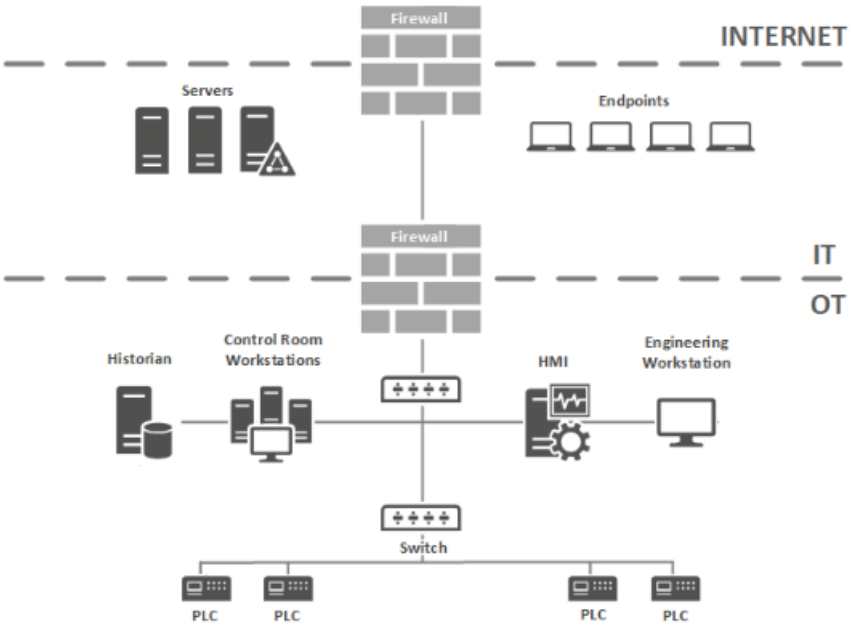


Figura 10 – Ativos em Redes Industriais

Adaptado de wizlynx group (2023).

2.5.6 Protocolo SNMP

O SNMP (Protocolo Simples de Gerenciamento de Rede) é amplamente utilizado para administrar redes em dispositivos como roteadores, *switches*, servidores e outros equipamentos de infraestrutura. Seu objetivo é permitir que os administradores de rede coletem informações, monitorem e controlem esses dispositivos de maneira centralizada. Segundo Cisco Systems (2004), o SNMP é um protocolo da camada de aplicação que facilita a troca de informações de gerenciamento entre dispositivos de rede. Ele faz parte da suíte de protocolos TCP/IP. A figura Figura 11 ilustra o funcionamento do protocolo SNMP.

Com base em Dias e Alves Jr (2001), alguns dos principais conceitos do SNMP, são:

- Agentes SNMP: São os dispositivos gerenciados que mantêm informações gerenciáveis na forma de variáveis gerenciadas. Os agentes são responsáveis por responder a solicitações de informações e executar ações de controle.
- Gerentes SNMP: São sistemas de monitoramento e gerenciamento que solicitam informações e enviam comandos para os agentes SNMP. Eles coletam dados dos dispositivos gerenciados e apresentam essas informações aos administradores.

- Variáveis gerenciadas: Representam os parâmetros ou valores que um agente SNMP pode monitorar ou controlar. Cada variável é identificada por um identificador único conhecido como *Object Identifier* (OID).
- Mensagens SNMP: Existem três tipos principais de operações suportadas pelo SNMP: *GET*, *SET* e *Trap*. A operação *GET* permite que os gerentes solicitem informações das variáveis gerenciadas dos agentes, enquanto a operação *SET* permite que os gerentes enviem comandos para modificar os valores das variáveis gerenciadas nos agentes, já a operação *TRAP* é utilizada para comunicar um evento, o agente comunica ao gerente o acontecimento de um evento, previamente determinado.
- MIB (Base de Informações de Gerenciamento): A MIB é uma estrutura de dados hierárquica que define as variáveis gerenciadas disponíveis em um dispositivo SNMP. As MIBs são usadas para organizar e identificar as informações que podem ser gerenciadas por meio do protocolo SNMP.

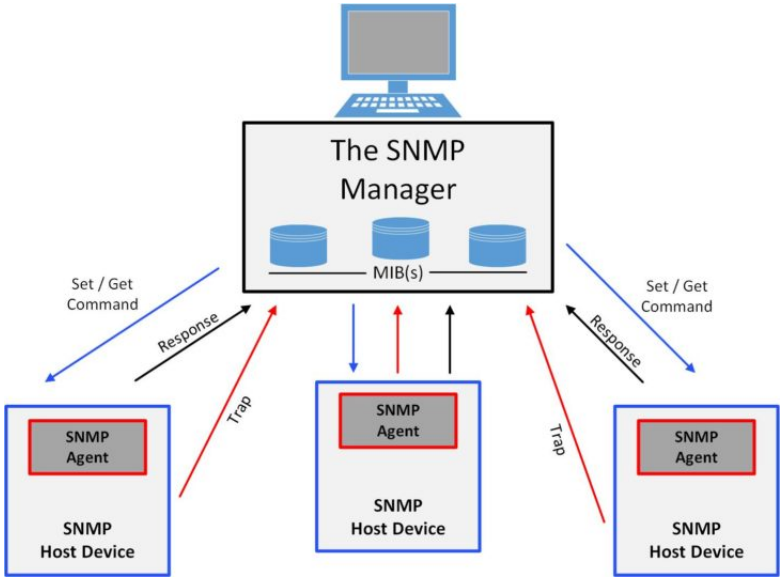


Figura 11 – Sistema SNMP

Fonte: Pecena (2023)

2.5.7 Protocolo SSH

A partir do trabalho de Lonvick e Ylonen (2006), entende-se que o protocolo SSH, também conhecido como *Secure Shell*, é um protocolo criptografado amplamente empregado para garantir comunicações seguras entre dois sistemas em uma rede. Essa tecnologia permite a transmissão segura de dados e a execução remota de comandos. A sua criação teve o propósito de substituir protocolos inseguros, como o *Telnet*, que não utilizavam criptografia, tornando-os vulneráveis a ataques de interceptação.

Ademais, segundo Macedo et al. (2018), o funcionamento do SSH se baseia em técnicas avançadas de criptografia, que garantem tanto a confidencialidade quanto a integridade dos dados durante a sua transmissão. Adicionalmente, o protocolo oferece recursos de autenticação para clientes e servidores, garantindo que somente partes autorizadas tenham acesso aos sistemas envolvidos. Alguns exemplos de *softwares* para conexão SSH incluem o OpenSSH e o PuTTY.

2.6 Cibersegurança

De forma simplificada, cibersegurança pode ser definida como o conjunto de práticas, tecnologias, políticas e procedimentos desenvolvidos para proteger sistemas de computadores, redes, dispositivos eletrônicos e dados contra ataques cibernéticos, danos, roubos e acessos não autorizados (STALLINGS, 2003).

Como a tecnologia operacional tem se tornado cada vez mais conectada à Internet, à outras redes e tecnologias, a cibersegurança para a TO é crucial para garantir a integridade, disponibilidade e confidencialidade das operações industriais. Além disso, a segurança desses sistemas é fundamental para prevenir danos físicos, impactos ambientais e até mesmo perdas financeiras significativas.

Com base na IEC62443 (2007-2018), algumas das práticas e medidas de cibersegurança comuns para tecnologia operacional incluem:

- Segmentação de rede: dividir a rede em zonas e limitar a comunicação apenas ao necessário para minimizar a exposição a ataques.
- Autenticação e controle de acesso: garantir que apenas usuários autorizados tenham acesso aos sistemas e dados críticos.
- Monitoramento e detecção de intrusões: utilizar ferramentas e sistemas de monitoramento para identificar atividades suspeitas ou maliciosas.
- Criptografia: proteger dados sensíveis por meio de criptografia para evitar interceptações não autorizadas.
- Atualizações regulares: manter os sistemas atualizados com as correções de segurança mais recentes e *patches* de *software*.
- Treinamento e conscientização: educar os funcionários sobre boas práticas de segurança e reconhecimento de ameaças cibernéticas.
- Resposta a incidentes: desenvolver planos e procedimentos para lidar com incidentes de segurança caso ocorram.

- Testes de segurança: realizar testes de penetração e avaliações de vulnerabilidade para identificar falhas e corrigi-las antes que sejam exploradas por invasores.

2.7 Gerenciamento de Redes

O gerenciamento ou administração de redes de computadores refere-se à organização e supervisão das atividades, monitoramento e utilização dos dispositivos de rede, tais como computadores, servidores, roteadores e dos recursos lógicos, como os protocolos TCP, UDP e IP. Esses elementos são distribuídos fisicamente em uma rede com o propósito de garantir a confiabilidade, um tempo de resposta aceitável e a segurança das informações que circulam na rede. Quanto às tarefas fundamentais abordadas pelo gerenciamento de redes, elas podem ser classificadas da seguinte maneira (MACEDO et al., 2018):

- Coleta de dados: refere-se à obtenção de informações abrangentes dos dispositivos conectados à rede, normalmente de forma automatizada, por meio de agentes de *software*.
- Diagnóstico: envolve o processo de identificação e análise dos dados coletados, com o objetivo de compreender e solucionar eventuais problemas.
- Ação ou Controle: após a identificação de um problema na rede de computadores, são tomadas medidas ou implementadas ações específicas para lidar com o problema em questão.

2.7.1 Monitoramento

Segundo Macedo et al. (2018), o monitoramento de rede pode ser definido basicamente como a observação de informações relevantes para o gerenciamento de uma rede de computadores e pode ser dividido em três categorias distintas:

- Monitoramento Estático: são acompanhados os elementos da rede em sua configuração atual, como as portas dos *switches*, os endereços IP em uso, entre outros parâmetros estáveis.
- Monitoramento Dinâmico: refere-se à coleta de dados em tempo real sobre o tráfego que circula na rede. Isso inclui informações sobre os dados que estão sendo transmitidos entre os dispositivos conectados, tornando-se uma valiosa fonte de *insights* dinâmicos.
- Monitoramento Estatístico: engloba dados estatísticos referentes à rede, como a quantidade de pacotes enviados e recebidos por uma determinada *interface*, o total de conexões estabelecidas por um computador, entre outros indicadores relevantes.

2.7.2 Controle

Macedo et al. (2018) afirmam, que para garantir a eficiência do gerenciamento de uma rede, é fundamental contar com um sistema de controle de rede adequado e eficaz. Essa parte do gerenciamento permite ajustar parâmetros e realizar ações em um sistema remoto de forma precisa e eficiente. Além disso, esse controle de rede deve ter algumas funções, como a definição da informação a configuração que será controlada, a inicialização e terminação de operações de serviços de rede e os relatórios de status de configuração.

Ademais, quanto ao controle de segurança aplicado aos dispositivos que constituem uma rede de computadores, as principais ameaças à segurança envolvem interrupção de serviços, interceptação de dados, alteração de informações e disfarce de atividades maliciosas. Resultando em três categorias de gerenciamento de segurança: manutenção das informações de segurança, controle de acesso aos recursos e gerenciamento do processo de criptografia (MACEDO et al., 2018).

2.8 Manutenção Preditiva

Nas redes de computadores industriais, a manutenção preditiva assume um papel muito importante, uma vez que essas redes são fundamentais para garantir a operação segura e eficiente dos processos industriais automatizados. Nesse contexto, a manutenção preditiva é empregada para antecipar e prevenir possíveis falhas em dispositivos e equipamentos industriais, assegurando a continuidade da operação e evitando paradas não programadas, que poderiam gerar prejuízos financeiros consideráveis. Veja a seguir uma breve descrição do termo:

> "A Manutenção Preditiva ou Condicionada surgiu na década de 70 como um conceito evoluído da manutenção preventiva sistemática em que, em vez de ações de manutenção em intervalos de tempo definidos para trocas de componentes, teremos ações de inspeção em intervalos de tempo definidos. Manutenção preditiva é aquela que indica as condições reais de funcionamento das máquinas com base em dados que informam os seus desgastes ou processo de degradação. Trata-se da manutenção que prediz o tempo de vida útil dos componentes das máquinas e equipamentos e as condições para que esse tempo de vida seja bem aproveitado, daí o nome manutenção preditiva ou condicionada"(SOUZA, 2013).

Com base em um relatório da Deloitte, Patil et al. (2022), alguns benefícios importantes da manutenção preditiva (PdM) incluem:

- Melhoria na expectativa de vida dos ativos, levando a redução nos gastos de capital

para substituição dos mesmos.

- Redução nos custos de horas extras devido à diminuição de reparos não planejados.
- Disponibilidade ideal de técnicos de manutenção qualificados e operadores em momentos de escassez de mão de obra.
- Melhor gerenciamento e previsibilidade de peças de reposição.
- Maior controle sobre o planejamento de produção/operações.
- Melhoria no equilíbrio entre trabalho e vida pessoal da equipe de manutenção.
- Melhoria na segurança da equipe de trabalho devido à redução de falhas nos ativos.

3 Ferramenta de Monitoramento Zabbix

O Zabbix é uma ferramenta atual, *open source* e compatível com várias plataformas, não requerendo pagamento de licenças, uma vez que é licenciado sob a GPLv2 (Licença Pública Geral GNU). A única versão disponível é considerada de categoria empresarial e é globalmente utilizada para monitorar a disponibilidade e o desempenho de aplicativos, ativos e serviços de rede (HORST; SANTOS PIRES; DÉO, 2015).

O Zabbix oferece muitas maneiras de monitorar diferentes aspectos da infraestrutura de rede e, de fato, praticamente qualquer coisa que você queira conectar a ele. Ele pode ser caracterizado como um sistema de monitoramento semi-distribuído com gerenciamento centralizado. Embora muitas instalações tenham um único sistema central, é possível usar monitoramento distribuído com *proxies*, e a maioria das instalações usará agentes Zabbix (REIS LIMA, 2014).

De acordo com Olups (2016), os principais recursos oferecidos pelo Zabbix são:

- Uma *interface web* centralizada e fácil de usar.
- Um servidor que funciona na maioria dos sistemas operacionais semelhantes ao *UNIX*, incluindo *Linux, AIX, FreeBSD, OpenBSD e Solaris.*
- Agentes nativos para a maioria dos sistemas operacionais semelhantes ao *UNIX* e versões do *Microsoft Windows.*
- Capacidade de monitorar diretamente dispositivos SNMP (SNMPv1, SNMPv2 e SNMPv3) e dispositivos IPMI.
- Capacidade de monitorar diretamente aplicações Java usando *Java Management Extensions* (JMX).
- Capacidade de monitorar diretamente instâncias do *vCenter* ou *vSphere* usando o *VMware API.*
- Recursos internos de gráficos e outras capacidades de visualização.

3.1 Arquitetura

O Zabbix adota uma arquitetura conhecida como *three-tier* (três camadas) para organizar seus serviços de rede. Essa estrutura é composta por três camadas distintas: aplicação, banco de dados e *interface web* (REIS LIMA, 2014). A Figura 12 ilustra a arquitetura do Zabbix.

A primeira camada, denominada de aplicação ou *back-end*, é responsável por coletar os dados provenientes dos ativos de rede. Nessa etapa, são reunidas informações relevantes para o monitoramento dos sistemas. A segunda camada corresponde ao banco de dados, que tem a tarefa de armazenar todas as informações coletadas pelo *back-end*. Esse repositório central contém os dados que serão posteriormente apresentados ao *front-end*. Por fim, a terceira camada é representada pela *interface web* ou *front-end*. Essa *interface* oferece acesso aos administradores para visualizarem e monitorarem as informações coletadas. Além disso, ela também fornece dados para aplicações que se conectam à API do Zabbix (OLUPS, 2016).

Com essa abordagem em três camadas, o Zabbix consegue organizar de forma eficiente todo o processo de monitoramento, permitindo que os administradores obtenham *insights* importantes sobre o desempenho dos ativos de rede e facilitem o gerenciamento geral do sistema.

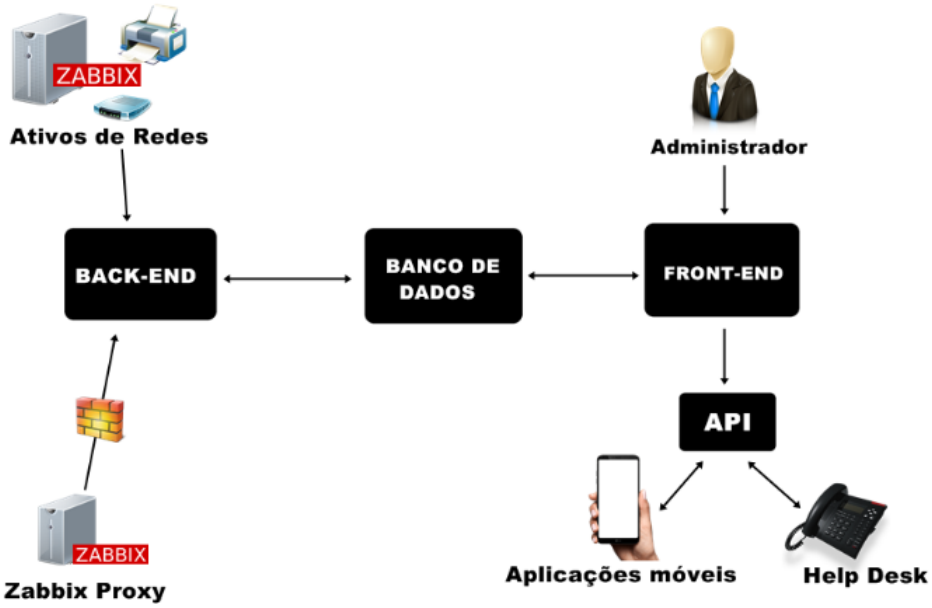


Figura 12 – Arquitetura do Zabbix

Fonte: Bernardo (2018)

De acordo com Reis Lima (2014), o núcleo do Zabbix foi construído utilizando a linguagem de programação C, enquanto a *interface* de usuário foi desenvolvida em PHP. Essa escolha de linguagens permite que o Zabbix tenha um desempenho sólido e eficiente no processamento dos dados coletados.

Além disso, o Zabbix foi projetado para ser compatível com os principais Sistemas Gerenciadores de Banco de Dados (SGBDs) disponíveis no mercado. Essa flexibilidade permite que os usuários escolham o banco de dados que melhor se adapta às suas necessidades

e infraestrutura (HORST; SANTOS PIRES; DÉO, 2015).

A partir da versão 1.8, o Zabbix passou a contar com uma API (*Interface* de Programação de Aplicativos) que possibilita a integração com outros sistemas. Isso significa que é possível conectar o Zabbix a diferentes aplicações, como sistemas de registro de chamados, tornando-o ainda mais versátil e útil para a gestão integrada de diversas ferramentas e processos. Essa integração amplia as possibilidades de uso do Zabbix, facilitando sua adaptação às necessidades específicas de cada ambiente de monitoramento (REIS LIMA, 2014).

3.2 Definições

De acordo com SIA (2021-2023), nesta seção será apresentado o significado de alguns termos comumente usados no Zabbix:

- *Hosts*: representam os ativos ou sistemas que serão monitorados. Podem ser servidores físicos, máquinas virtuais, roteadores, *switches*, impressoras, entre outros.
- Itens: são os parâmetros individuais que serão monitorados em um *host*. Eles podem ser métricas como uso de CPU, utilização de memória, tráfego de rede, disponibilidade de serviços, entre outros.
- *Triggers*: são condições configuradas para determinar quando um evento deve ser acionado com base nos valores dos itens monitorados. Quando um item ultrapassa um limite definido, o *trigger* é acionado e um evento é registrado.
- Eventos: representam ocorrências importantes no sistema monitorado, como alertas de problemas ou mudanças de status.
- Ações: são respostas automáticas configuradas para serem executadas quando um evento é acionado. Por exemplo, enviar notificações por e-mail, reiniciar um serviço ou executar um *script*.
- Gráficos: permitem visualizar o histórico de valores de um ou mais itens ao longo do tempo. São úteis para acompanhar tendências e identificar padrões de comportamento.
- *Dashboard*: são painéis personalizáveis que podem conter vários gráficos, itens, *widgets* e mapas para fornecer uma visão geral do ambiente monitorado.
- *Proxies*: são agentes intermediários que podem ser utilizados para distribuir a carga de monitoramento e coletar dados de *hosts* em redes remotas.

- *Templates*: são modelos pré-configurados que podem ser aplicados a *hosts* para facilitar o processo de monitoramento. Eles contêm itens, *triggers*, gráficos e outros elementos predefinidos.
- *Discovery Rules*: permitem descobrir automaticamente novos *hosts* e serviços em uma rede e adicioná-los ao monitoramento com base em critérios definidos.
- Escalas de Disponibilidade (SLAs): são métricas para monitorar a disponibilidade e o tempo de resposta dos serviços, permitindo medir o cumprimento de acordos de nível de serviço.
- API do Zabbix: permite a utilização do protocolo JSON RPC para criar, atualizar e buscar objetos Zabbix (como *hosts*, itens, gráficos e outros) ou executar qualquer outra tarefa personalizada.
- *Zabbix Server*: um processo central do *software* Zabbix que realiza monitoramento, interage com *proxies* e agentes Zabbix, calcula gatilhos, envia notificações, um repositório central de dados.
- *Zabbix Agent*: um processo implantado em alvos de monitoramento para monitorar ativamente recursos e aplicativos locais.

3.3 Segurança

A *interface web* do Zabbix pode ser acessada por meio de uma conexão segura usando *secure sockets layer* (SSL), o que garante a segurança das interações entre os usuários e o servidor. Todos os componentes do Zabbix podem operar como usuários desprivilegiados, o que é especialmente importante para os agentes nativos. Além disso, executar os *daemons* do Zabbix com privilégios requer etapas adicionais (GONÇALVES, 2020).

Os componentes do Zabbix se comunicam entre si e só aceitam conexões de endereços IP autorizados, rejeitando automaticamente outras conexões. O suporte à criptografia permite proteger as comunicações entre os diferentes componentes do Zabbix, como servidor Zabbix, *proxies*, agentes e utilitários de linha de comando, usando o protocolo de segurança *Transport Layer Security* (TLS). A criptografia pode ser baseada em certificados ou em chave pré-compartilhada, sendo opcional e configurável para cada componente individualmente. Isso adiciona uma camada adicional de segurança para garantir a integridade e confidencialidade das informações transmitidas entre os elementos do Zabbix (GONÇALVES, 2020).

4 Projeto Proposto

4.1 Apresentação do Ambiente

O ambiente proposto é de extrema relevância para a empresa mineradora, pois é a fonte de todo o minério de ferro utilizado para a produção das pelotas, matéria-prima na produção de aço pela indústria siderúrgica. Portanto, além da importância do ambiente, existem desafios significativos que justificam a implementação deste trabalho:

1. Diagnóstico de problemas: a arquitetura de rede da mina é pouco conhecida, e sua extensa área territorial dificulta a identificação rápida de problemas. Como resultado, em caso de falhas em ativos (*switches*, rádios, CLPs, entre outros), o tempo de resposta é bastante lento, o que pode acarretar em atrasos no *lead time* do processo.

2. Falta de monitoramento de ativos: a ausência de monitoramento dos ativos impede a adoção de uma abordagem preditiva. O monitoramento proativo e em tempo real, é essencial para identificar e resolver problemas, antes que estes se tornem graves, garantindo a eficiência e a segurança das operações.

O controle e a operação dos processos da empresa mineradora, são realizados por meio do Centro de Operações Integradas (COI). Logo, para que o COI opere de forma eficiente, é imprescindível contar com uma estrutura de rede adequada, segura e robusta. Uma rede bem projetada garantirá a estabilidade necessária para o controle e a operação dos processos de forma contínua e confiável. Além disso, a segurança da rede é fundamental para proteger os dados e informações sensíveis da empresa contra ameaças cibernéticas, ainda mais em um abiente bastante exposto.

4.2 Delimitação do Monitoramento

A delimitação de monitoramento refere-se ao processo de especificar quais itens, *hosts* ou grupos serão monitorados pelo Zabbix. Essa delimitação é importante para garantir que o Zabbix colete e acompanhe somente os dados relevantes para o usuário, evitando sobrecarregar o sistema com informações desnecessárias.

Neste trabalho, os *hosts* a serem monitorados pelo Zabbix são:

- *Switches*;
- Servidores;

- Rádios;
- CLPs;
- IHMs;
- *COMBricks*;
- OWS (Estações de Operação);
- EWS (Estações de Engenharia).

4.3 Instalação e Configuração

A instalação do Zabbix requer certos requisitos de memória e armazenamento, no entanto, é importante notar que a quantidade necessária de memória e espaço em disco dependerá diretamente do número de *hosts* e parâmetros que serão monitorados (SIA, 2021-2023). Caso seja necessário manter um histórico extenso dos parâmetros monitorados, é recomendável reservar alguns *gigabytes* de espaço para garantir que haja disponibilidade suficiente para o banco de dados.

Com isso, foi disponibilizado pela equipe de infraestrutura de automação da empresa de mineração uma máquina virtual (VM) para instalação do *Zabbix Server e Agent*. Essa máquina virtual, é composta por 4GB de memória RAM e um *hard disk* com espaço de 120GB de armazenamento. O sistema operacional (SO) utilizado para instalação foi o *Ubuntu Server Linux (64 bits)*. A versão 5.0.24 do Zabbix foi instalada em inglês e foi utilizada como base instrutiva a documentação disponibilizada pelo próprio Zabbix. A Figura 13 ilustra algumas informações referentes a máquina virtual criada.

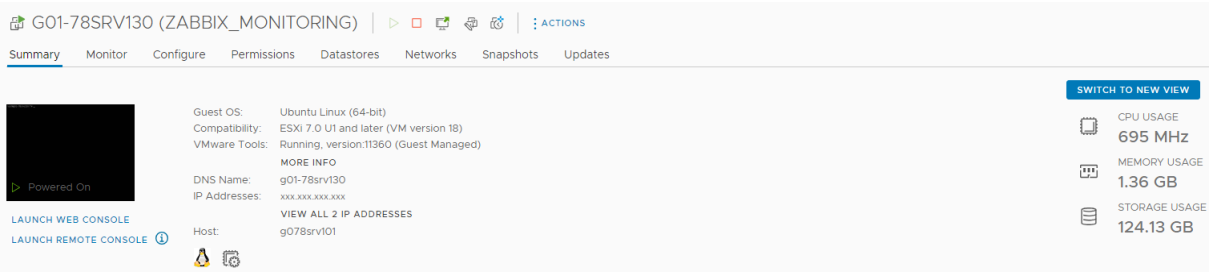


Figura 13 – Resumo de Informações da VM

Fonte: Própria Autora

Após as etapas de instalação e configuração do *Zabbix Server*, do *Zabbix Agent* e da *interface web*, o sistema está pronto para iniciar o monitoramento, a *interface* do

Zabbix é acessada por meio de um *browser*, através de um *link*, que redireciona para a tela de *login* do Zabbix, vide Figura 14.

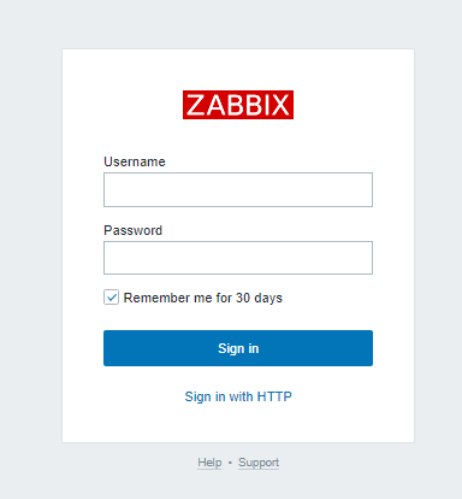


Figura 14 – Tela de Login do Zabbix

Fonte: Própria Autora

Após realizar o *login*, com *username* e senha, tem-se acesso ao *dashboard*, ilustrado na Figura 15, onde são exibidas informações do sistema. Algumas informações recentes sobre os *hosts* e alguns mapas de monitoramento. Vale lembrar que o *dashboard* do Zabbix, pode ser personalizado conforme as preferências do usuário.

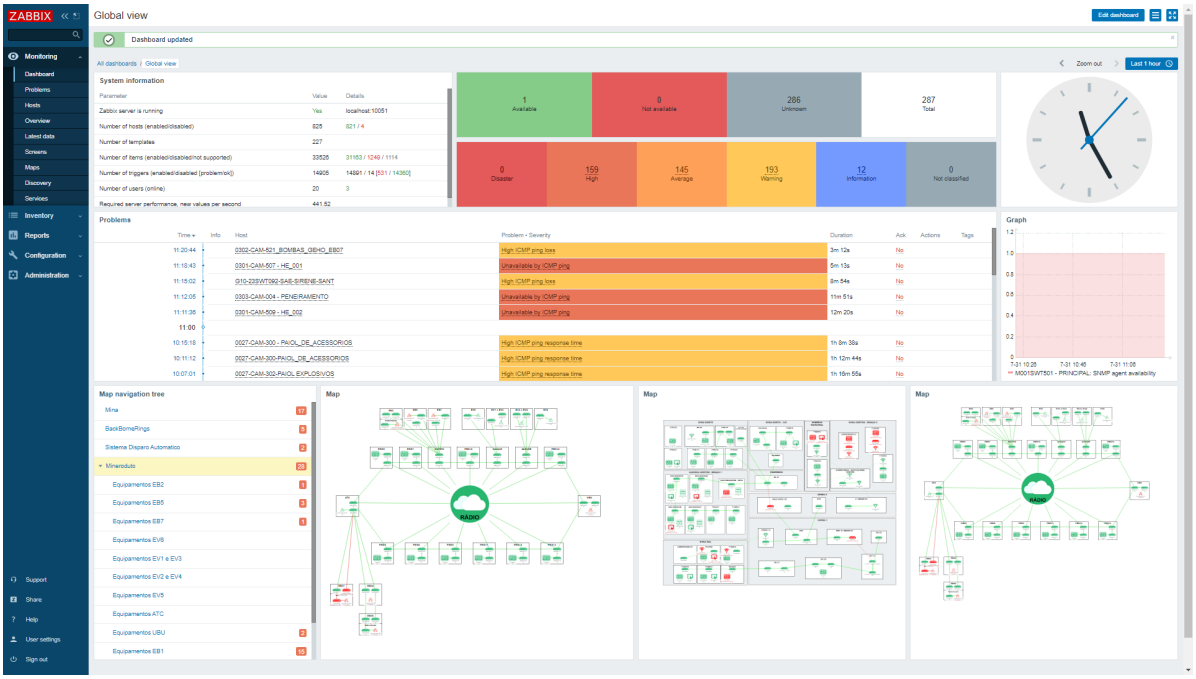


Figura 15 – Dashboard criado no Zabbix

Fonte: Própria Autora

4.3.1 *Hosts*

Para criar um *host* no Zabbix, ilustrado na Figura 16, realiza-se os seguintes passos:

- Acesse a *interface web* do Zabbix e faça *login* com suas credenciais de administrador.
- Clique em *"Configuration"* no menu lateral e selecione *"Hosts"*.
- Clique no botão *"Create Host"* para adicionar um novo *host*.
- Preencha os detalhes básicos, como o nome do *host*, a *interface* (IP ou DNS do *host* monitorado) e o *group* de *hosts* ao qual ele pertence.
- Escolha o *template* que será aplicado a esse *host*, conforme Figura 17, contendo os itens, *triggers* e gráficos pré-configurados.
- Configure as macros (se necessário) para personalizar as configurações do *host*.
- Defina o modo de monitoramento, que pode ser *"Zabbix Agent"*, *"SNMP"* ou outros, dependendo da circunstância.
- Salve as configurações do *host*.

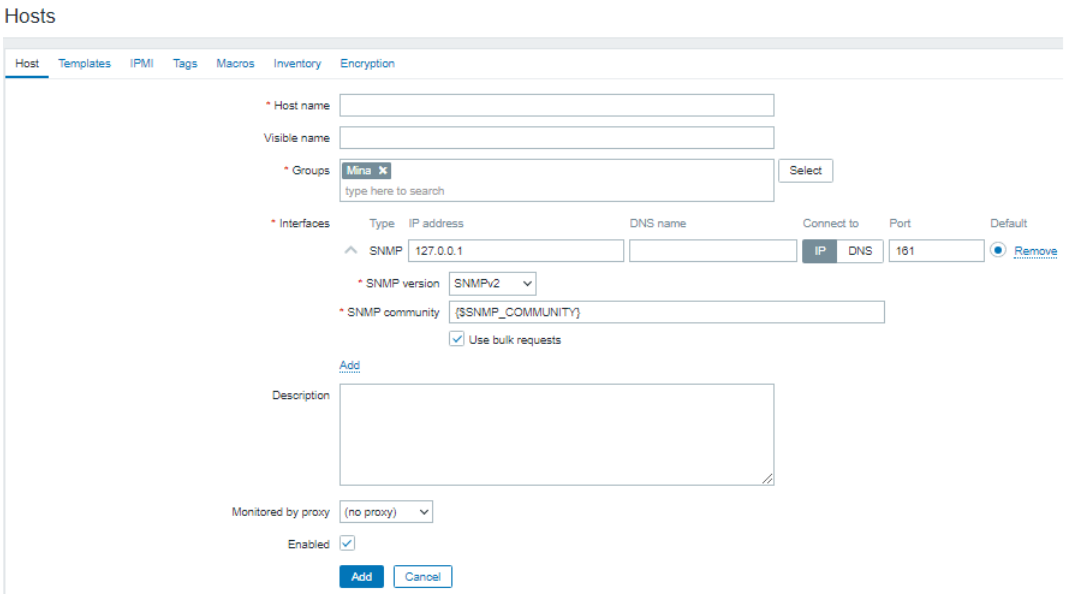


Figura 16 – Formulário para Criar um Host

Fonte: Própria Autora

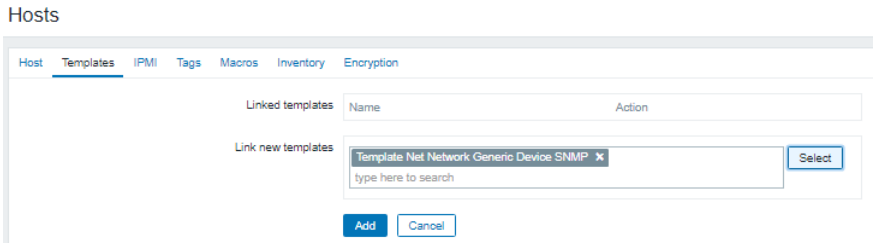


Figura 17 – Associação de Templates ao Host

Fonte: Própria Autora

Após concluir esses passos, o *host* estará configurado, e o monitoramento será ativado com base nas configurações definidas. Porém, é fundamental garantir que o agente ou protocolo de monitoramento esteja configurado corretamente no *host* para que todas as informações sejam coletadas de maneira adequada pelo Zabbix.

Quando um *template* é associado a um *host*, todas as configurações definidas no *template* são herdadas pelo *host*. O *host* passa a utilizar as configurações do *template* para monitoramento, e com isso, é possível gerenciar e fazer alterações em todas as instâncias associadas a esse *template* de uma só vez. Isso simplifica o processo de manutenção e personalização das configurações em diversos dispositivos ao mesmo tempo. A Figura 18 ilustra alguns *hosts* com os *templates* associados.

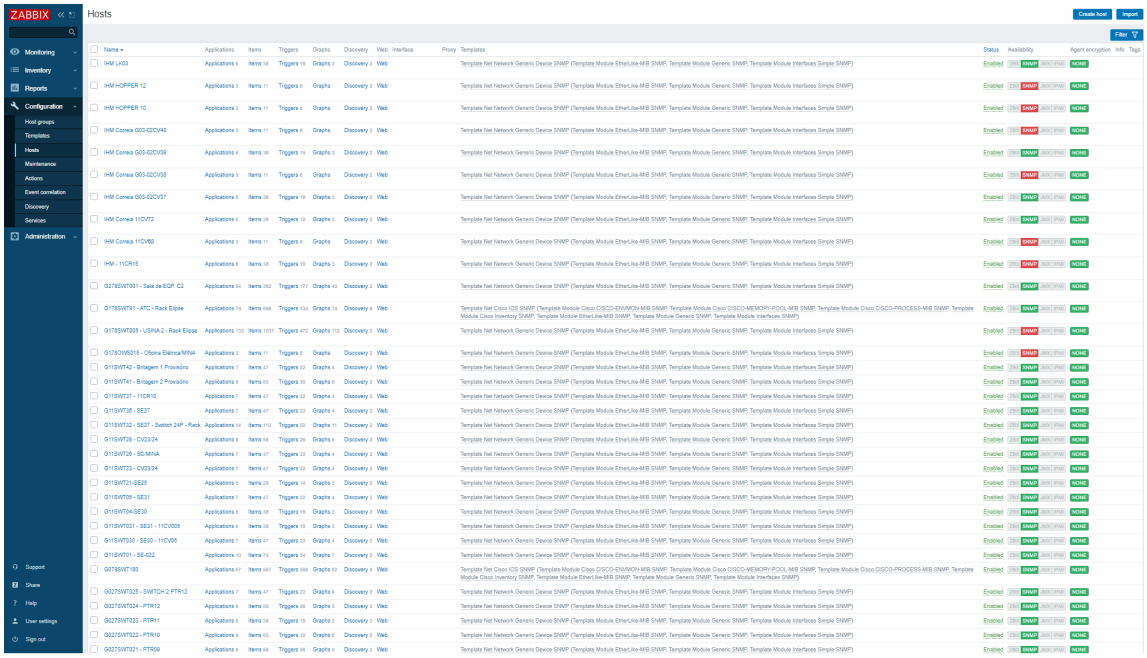


Figura 18 – Alguns Hosts com os Templates Associados

Fonte: Própria Autora

4.3.2 *Host Groups*

No Zabbix, um *"Host Group"* (Grupo de *Hosts*) é uma maneira de agrupar e organizar *hosts* que possuem características ou funções semelhantes. Essa abordagem facilita a gestão e configuração do monitoramento, especialmente em ambientes com um grande número de ativos. Ao agrupar *hosts* com características comuns em um único grupo, é possível aplicar configurações e políticas de monitoramento de forma mais eficiente e simplificada.

Na Figura 19 é ilustrado o formulário para criação de um *host group* e na Figura 20, alguns *host groups* criados.

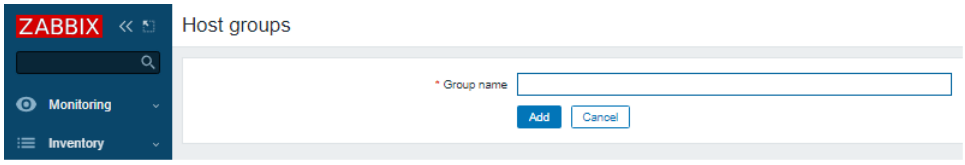


Figura 19 – Formulário para Criar um Host Group

Fonte: Própria Autora

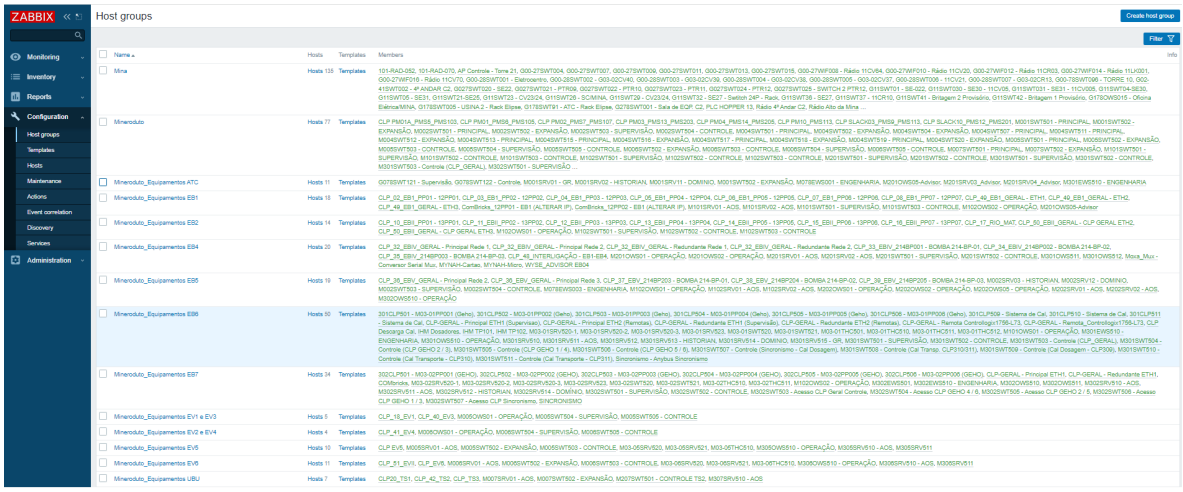


Figura 20 – Host Groups

Fonte: Própria Autora

Depois de criar o grupo de *hosts*, pode-se realizar a atribuição de *hosts* a ele durante a configuração do *host* ou modificando-o posteriormente.

4.3.3 *Maps*

A utilização de mapas no Zabbix é uma forma eficiente de visualizar a topologia da infraestrutura de rede. Os mapas ajudam a entender as relações entre os dispositivos monitorados e a identificar problemas/falhas de forma mais rápida e eficaz.

Para criar um mapa no Zabbix, primeiro é neccessário clicar em *"Monitoring"* no menu lateral e selecionar a opção *"Maps"*. Logo em seguida, clique em *"Create Map"*, forneca as informações do mapa, conforme Figura 21 e após a criação do mesmo, arraste os ícones dos *hosts* ou redes para o mapa, ilustrado na Figura 22. Utilize linhas para representar as conexões entre os elementos e personalize os mesmos com informações relevantes, como por exemplo, o status dos *hosts*. Após tudo pronto, salve o mapa.

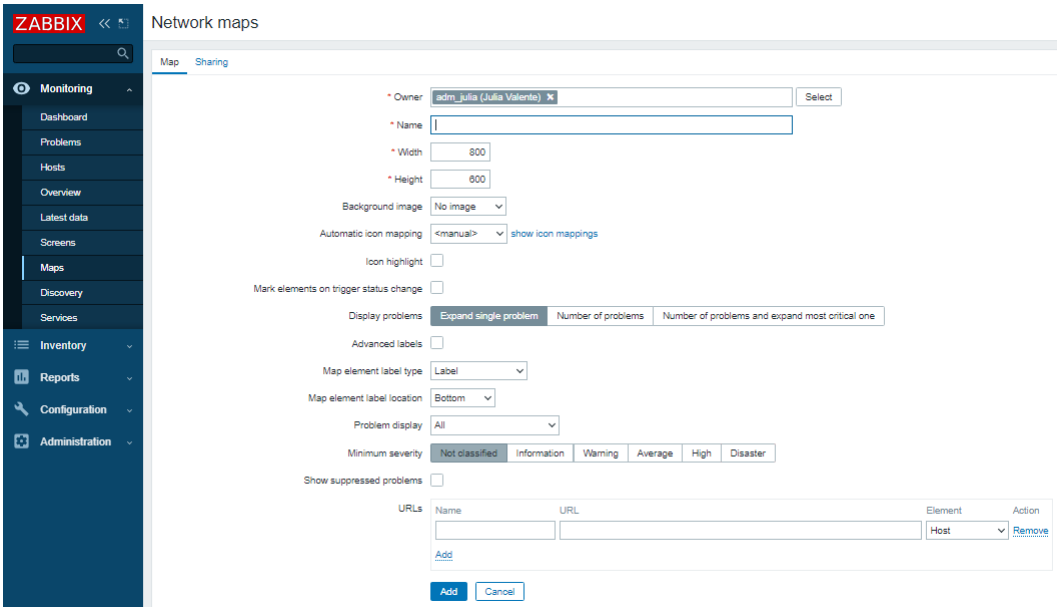


Figura 21 – Formulário para Criar um Mapa no Zabbix

Fonte: Própria Autora

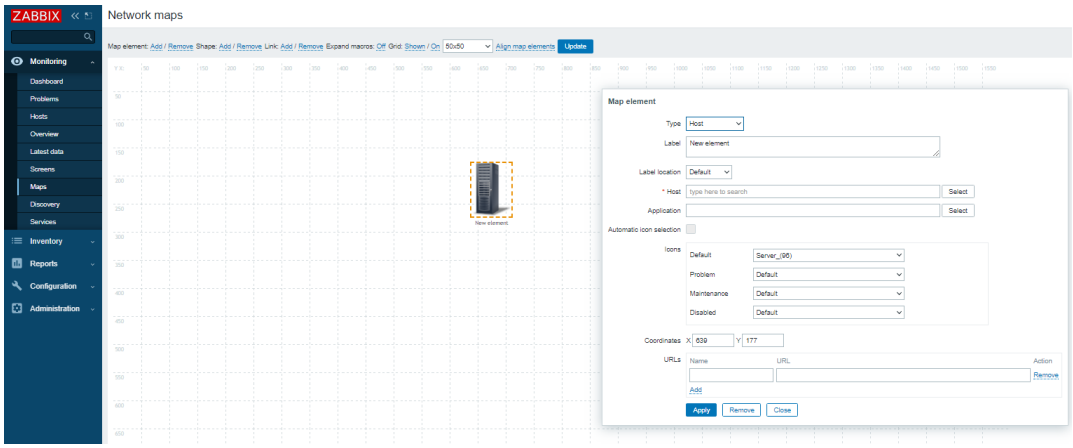


Figura 22 – Formulário para Configurar um Elemento no Mapa

Fonte: Própria Autora

Uma vez que o mapa é criado, o mesmo pode ser acessado por meio do menu *"Monitoring"* no Zabbix, exemplos de mapas criados são apresentados na Figura 23.

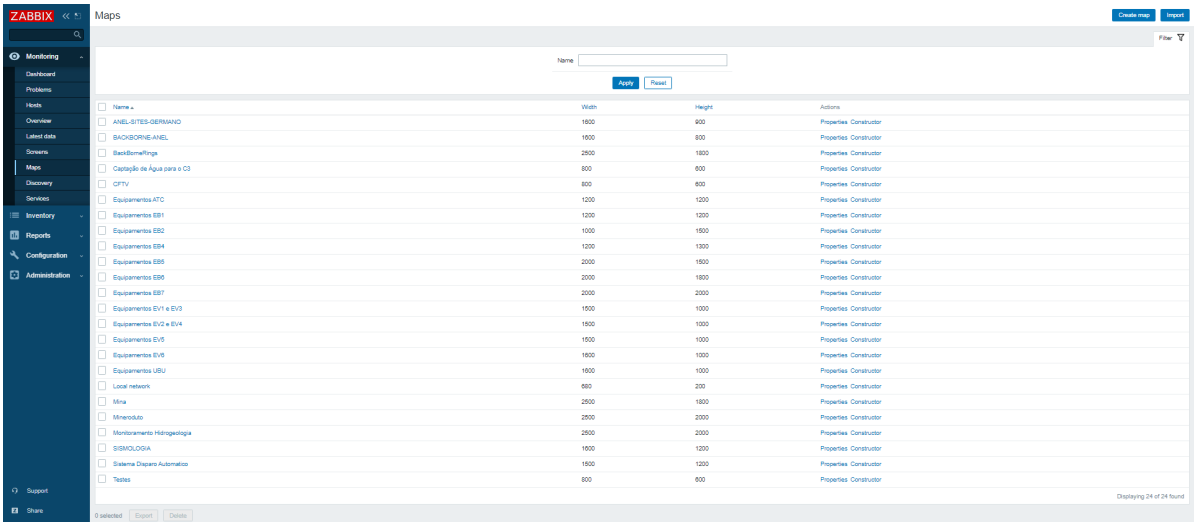


Figura 23 – Mapas Criados

Fonte: Própria Autora

4.3.4 *Users*

A criação de usuários no Zabbix é fundamental para permitir que diferentes pessoas ou equipes tenham acesso à *interface* do Zabbix com permissões específicas.

Para criar um usuário no Zabbix, primeiramente acesse *"Administration"* no menu lateral e depois *"Users"*. Clique em *"Create User"* e preencha o formulário de cadastro do usuário, com detalhes como: nome, sobrenome, alias, nome de usuário e senha. Escolha o grupo ao qual o usuário pertencerá para definir permissões e acesso, configure as permissões, atribuindo funções específicas e restringindo acesso se necessário. É possível também, definir outras configurações, como idioma preferido e autenticação, conforme Figura 24. Após finalizar, clique em *"Add"* para finalizar a criação do usuário.

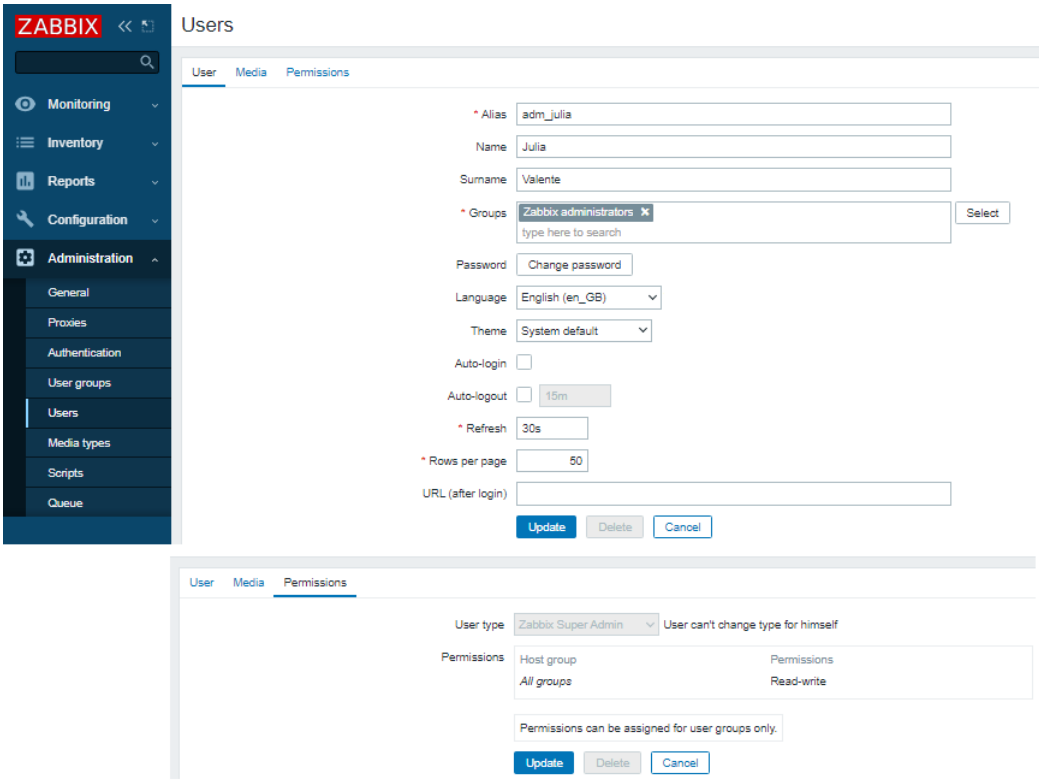


Figura 24 – Criando um Usuário

Fonte: Própria Autora

Após a cofiguração, o novo usuário estará disponível na lista de usuários, e ele poderá acessar a *interface* do Zabbix com as permissões e configurações específicas atribuídas a ele.

4.4 Monitoramento *Web*

Primeiramente, para poder realizar o monitoramento *online* dos ativos, foi necessário realizar algumas etapas, para que fosse possível obter um monitoramento seguro e eficiente, estas etapas são:

1. Desenhar a arquitetura de rede atual da Mina: com o intuito de identificar a localização e disposição dos ativos, bem como suas conexões. A análise da arquitetura de rede, permitirá compreender a topologia da rede e identificar possíveis gargalos, pontos de falha e áreas de melhoria. A Figura 25 ilustra a arquitetura de rede atual da Mina.

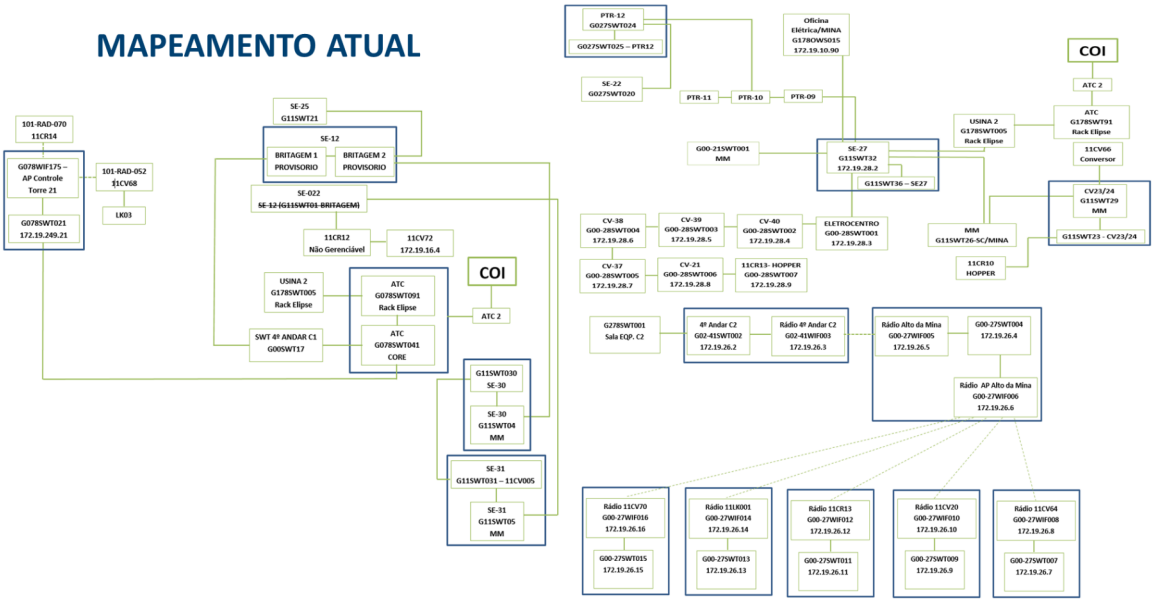


Figura 25 – Mapeamento da Arquitetura de Rede da Mina

Fonte: Própria Autora

2. *Switches Hardening*: com o intuito de garantir a segurança e a eficiência da rede. Algumas das medidas adotadas são: controle de acesso, adequação de IPs, uso de senhas de maior complexidade, desativação das portas não utilizadas, realizar a identificação adequada das portas, entre outros, ilustrado na Figura 26.

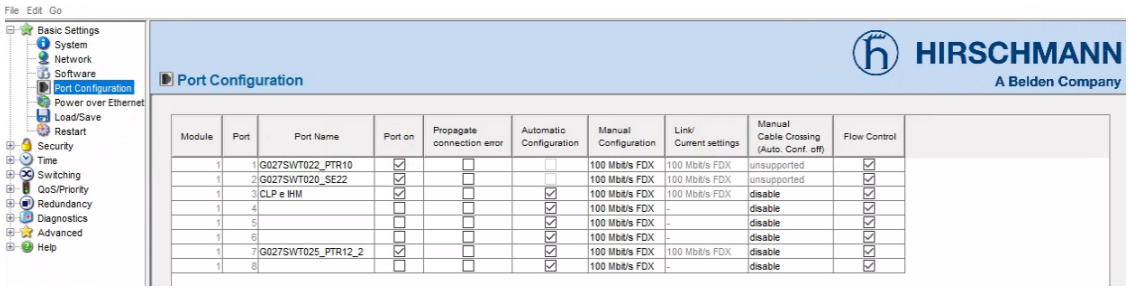


Figura 26 – Controle das Portas de um Switch

Fonte: Própria Autora

Anteriormente, o monitoramento da rede era realizado através da ferramenta WhatsUp Gold. Apesar de ser uma ótima ferramenta, a mesma apresentava um alto custo de licenciamento para a empresa, o que acabou motivando o interesse pelo Zabbix, uma vez que o mesmo é um *software* gratuito. O monitoramento da rede apresentava diversas deficiências, com um grande número de ativos em *off*, resultando em falta de monitoração, mapeamento desatualizado e interligações incorretas ou inexistentes, conforme ilustrado na

Figura 27. Essas falhas prejudicavam significativamente a capacidade de atuação preditiva e aumentavam consideravelmente o tempo de resposta em caso de falhas. Era uma tarefa árdua identificar a localização dos ativos em campo e entender sua situação operacional.

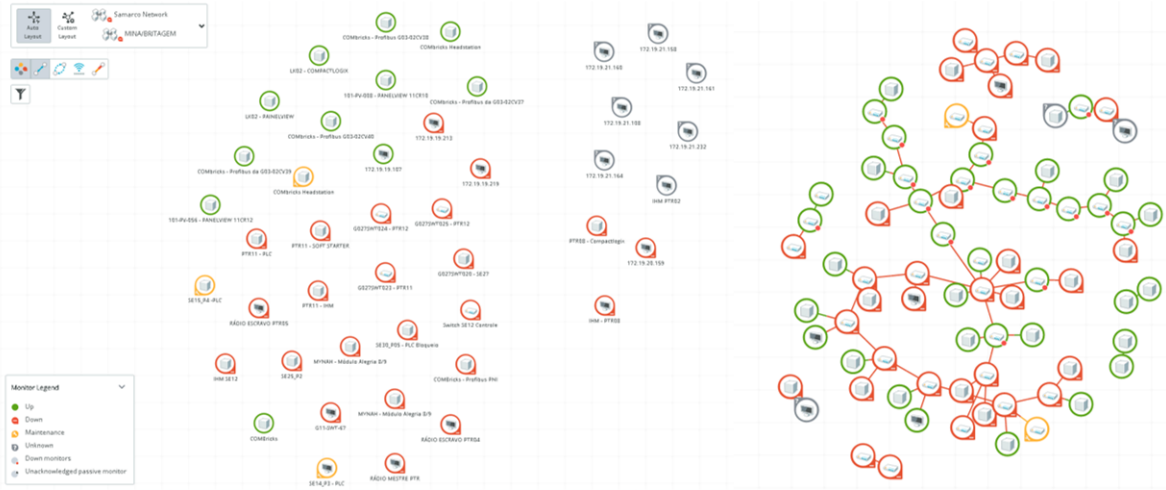


Figura 27 – Monitoramento da Rede da Mina: Anteriormente

Ativos em Verde = On, Vermelho = Off, Amarelo = Manutenção e Cinza = Desconhecido.

Fonte: Própria Autora

Atualmente, o mapeamento e monitoramento dos ativos da mina no Zabbix estão em um estado muito mais avançado. Foi criado um mapa, referente a toda a rede da mina, conforme pode ser visualizado na figura 28. A estrutura foi aprimorada para proporcionar clareza, intuição e organização, facilitando a supervisão das informações das interfaces e a conectividade dos equipamentos na rede.

A nova configuração no Zabbix permite uma visualização mais abrangente e detalhada do *status* de cada ativo, o que é extremamente valioso para a equipe de monitoramento e para a automação. Com a *interface* mais intuitiva, os dados são acessados com facilidade e rapidez, tornando o processo de identificação de problemas e a tomada de decisões mais ágil.

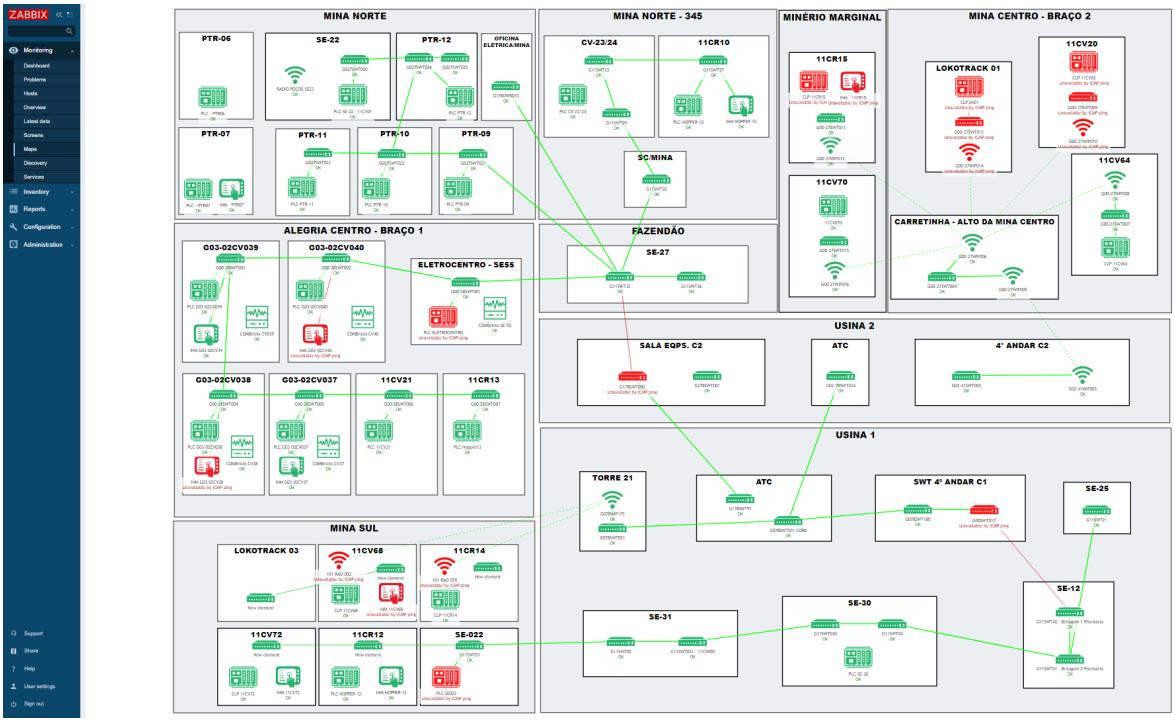


Figura 28 – Monitoramento da Rede da Mina: Atualmente

Fonte: Própria Autora

Além do monitoramento abrangente da arquitetura de rede da Mina, foi possível implementar a supervisão de várias métricas importantes nos ativos. Essas métricas fornecem *insights* valiosos sobre o desempenho e a saúde de cada dispositivo. Algumas dessas métricas incluem:

1. *Throughput* (Taxa de Transferência): foi acompanhado de perto a taxa de transferência de dados em cada ativo, o que permitiu identificar gargalos e garantir que o fluxo de informações ocorresse de maneira eficiente. Vide Figura 29.

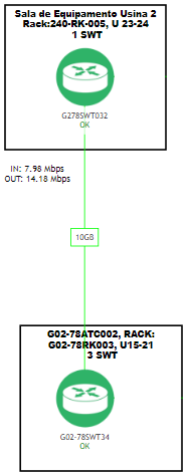


Figura 29 – Monitoramento de Throughput

Fonte: Própria Autora

2. Temperatura: o monitoramento da temperatura é essencial para prevenir o superaquecimento, um dos principais fatores que podem prejudicar o desempenho e a vida útil dos ativos, ilustrado na Figura 30.

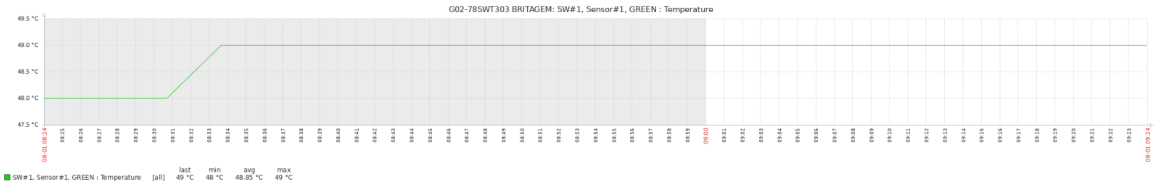


Figura 30 – Monitoramento da Temperatura de um Switch

Fonte: Própria Autora

3. *Network traffic* (Tráfego de Rede): a supervisão do tráfego de rede fornece uma visão clara sobre a quantidade de dados que estão sendo transmitidos em cada ponto da rede, isso permite a adoção de medidas para otimização do desempenho e asseguramento da qualidade da rede. Vide Figura 31.

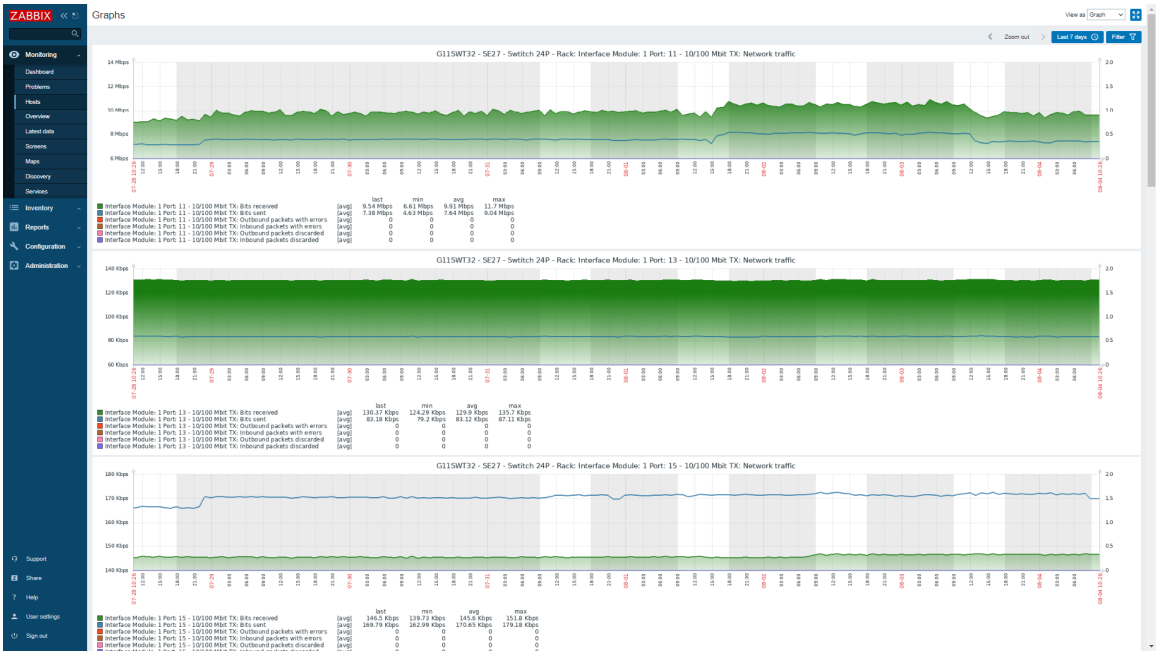


Figura 31 – Monitoramento do Tráfico de Rede de um Switch

Fonte: Própria Autora

4. *ICMP Ping*: foi realizado o monitoramento do *ICMP Ping* a fim de verificar a conectividade e a latência dos ativos. Essa abordagem possibilita a identificação de problemas de conectividade e latência em tempo real, segue exemplo na Figura 32.

Figura 32 – Relatório de Disponibilidade: ICMP Ping

Fonte: Própria Autora

5. *Action log* (Registro de Ações): responsável por manter um registro detalhado das ações realizadas no zabbix, isso auxilia na obtenção de uma compreensão mais aprofundada dos eventos, além de simplificar a análise em situações de problemas ou incidentes, conforme Figura 33.

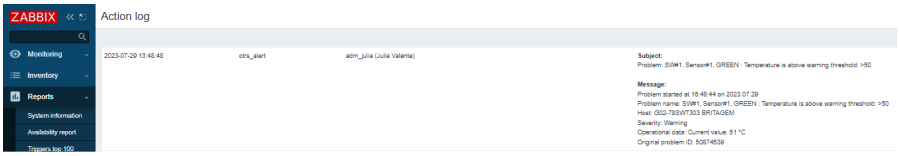
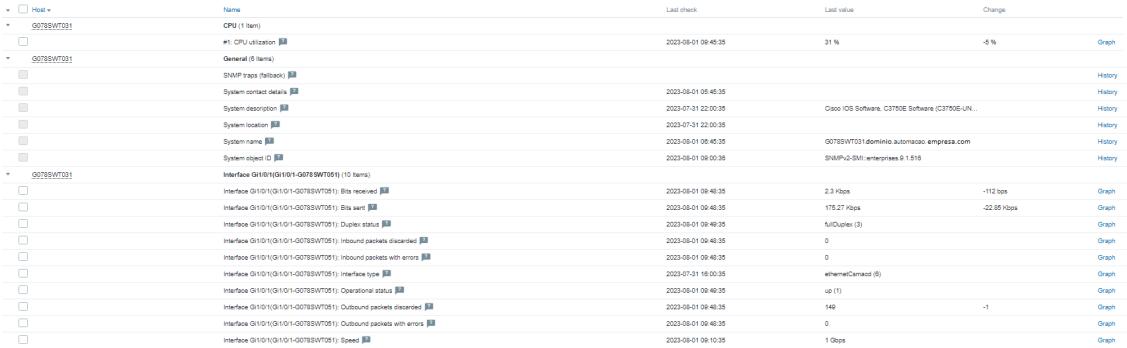


Figura 33 – Action Log: Problema de Temperatura

Fonte: Própria Autora

6. Utilização da CPU: a utilização da CPU em cada ativo foi monitorada de perto, possibilitando a identificação precoce de possíveis gargalos de processamento e a implementação de ações corretivas. Vide Figura 34.



Host	Name	Last check	Last value	Change	
G078SWT031	**CPU** (1 Item)				
	#1: CPU utilization	2023-08-01 09:45:35	31 %	-5 %	Graph
G078SWT031	**General** (6 Items)				
	SNMP traps (fallback)				History
	System contact details	2023-08-01 05:45:35			History
	System description	2023-07-31 22:00:35	Cisco IOS Software, C3750E Software (C3750E-UN...		History
	System location	2023-07-31 22:00:35			History
	System name	2023-08-01 05:45:35	G078SWT031.dominio.automacao.empresa.com		History
	System object ID	2023-08-01 09:00:36	SNMPv2-SMI::enterprises.9.1.516		History
G078SWT031	**Interface Gi1/0/1(Gi1/0/1-G078SWT051)** (10 Items)				
	Interface Gi1/0/1(Gi1/0/1-G078SWT051): Bits received	2023-08-01 09:46:35	2.3 Kbps	-112 bps	Graph
	Interface Gi1/0/1(Gi1/0/1-G078SWT051): Bits sent	2023-08-01 09:46:35	175.27 Kbps	-22.85 Kbps	Graph
	Interface Gi1/0/1(Gi1/0/1-G078SWT051): Duplex status	2023-08-01 09:46:35	fullDuplex (3)		Graph
	Interface Gi1/0/1(Gi1/0/1-G078SWT051): Inbound packets discarded	2023-08-01 09:46:35	0		Graph
	Interface Gi1/0/1(Gi1/0/1-G078SWT051): Inbound packets with errors	2023-08-01 09:46:35	0		Graph
	Interface Gi1/0/1(Gi1/0/1-G078SWT051): Interface type	2023-07-31 16:00:35	ethernetCsmacd (6)		Graph
	Interface Gi1/0/1(Gi1/0/1-G078SWT051): Operational status	2023-08-01 09:46:35	up (1)		Graph
	Interface Gi1/0/1(Gi1/0/1-G078SWT051): Outbound packets discarded	2023-08-01 09:46:35	149	-1	Graph
	Interface Gi1/0/1(Gi1/0/1-G078SWT051): Outbound packets with errors	2023-08-01 09:46:35	0		Graph
	Interface Gi1/0/1(Gi1/0/1-G078SWT051): Speed	2023-08-01 09:10:35	1 Gbps		Graph

Figura 34 – Dados mais Recentes de um Switch

Fonte: Própria Autora

Essas métricas monitoradas nos permite uma visão holística do desempenho da rede e dos ativos individuais. Com base nas informações coletadas, pode-se tomar decisões, antecipar possíveis problemas e garantir a estabilidade e eficiência do ambiente de rede como um todo. Esse monitoramento avançado é fundamental para manter a infraestrutura de rede da automação funcionando de maneira confiável e otimizada.

Para agregar ainda mais valor e aumentar o monitoramento das infraestrturas, além do ambiente proposto, também foi realizada a implementação do monitoramento em outros ambientes essenciais para a empresa de mineração, usando o Zabbix. Isso englobou o monitoramento da rede dos Minerodutos (Figura 35), um componente vital para o processo produtivo da empresa, e o *Backbone* (Figura 36) do site de operações, que desempenha um papel fundamental na conectividade e disponibilidade dos serviços da automação.

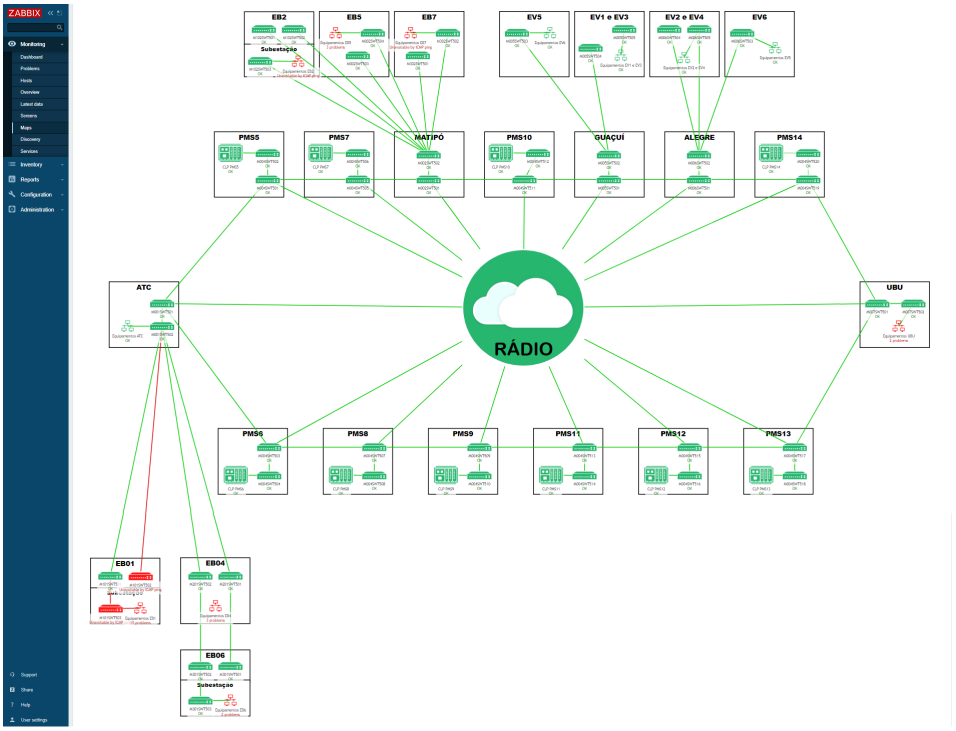


Figura 35 – Monitoramento do Mineroduto

Fonte: Própria Autora

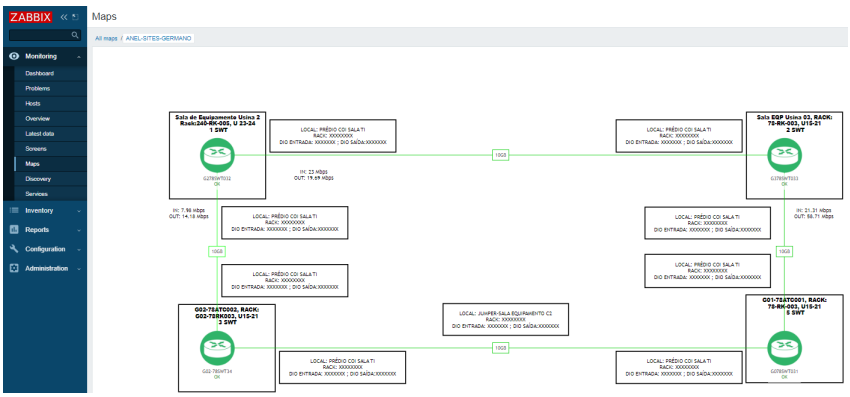


Figura 36 – Monitoramento do Backbone

Fonte: Própria Autora

A jornada com o Zabbix tem sido simultaneamente desafiadora e satisfatória. Sua implementação tem desempenhado um papel fundamental no monitoramento dos ativos da rede de automação da empresa, e seu alcance já se estende de forma considerável, uma vez que novos ambientes estão sendo implementados no mesmo. O intuito da empresa, é monitorar toda a sua rede de automação por meio da ferramenta Zabbix e gradativamente este objetivo vem sendo alcançado.

5 Conclusão

Este trabalho teve como objetivo realizar um estudo de caso abordando a utilização da ferramenta Zabbix para monitorar ativos em uma infraestrutura de rede de automação. Os objetivos específicos foram alcançados, permitindo conhecer e testar alguns dos recursos ofertados pelo Zabbix, ampliando o conhecimento sobre o *software* e investigando a contribuição do mesmo com a cibersegurança.

A implementação do Zabbix proporcionou um maior controle na identificação de falhas na infraestrutura de rede, permitindo um diagnóstico mais eficiente e auxiliando na prevenção de possíveis problemas. Com a utilização desta ferramenta, foi possível criar um sistema de monitoramento avançado, robusto, capaz de monitorar ativos em uma rede de automação e disponibilizar informações sobre os mesmos em tempo real.

A ferramenta se mostrou uma solução valiosa para garantir a segurança da infraestrutura de rede ao fornecer recursos de monitoramento e alertas que permitem a detecção rápida de anomalias como, tráfego incomum e picos de atividade, que podem indicar uma violação de segurança. Com isso, é possível a detecção precoce de incidentes e a implementação de medidas corretivas para proteger a infraestrutura de rede de TO. Além disso, o conhecimento adquirido sobre o Zabbix e seus recursos durante a elaboração desde trabalho, oferece um benefício duradouro, possibilitando a utilização efetiva da ferramenta para futuras expansões e melhorias na segurança da empresa.

Em suma, a utilização do Zabbix demonstrou ser uma medida eficaz para garantir a segurança da rede e melhorar a identificação de falhas, podendo dessa forma, aplicar a manutenção preditiva. O estudo de caso realizado neste trabalho serve como um exemplo concreto dos benefícios que podem ser alcançados ao adotar essa ferramenta de monitoramento em infraestruturas de rede de computadores, especialmente em setores críticos, como a automação em uma empresa do ramo da mineração.

Os resultados obtidos podem servir de base para futuros trabalhos, como a integração do Zabbix com uma plataforma interativa de visualização e análise de dados, a configuração da descoberta automática de *host*, a implementação de alertas avançados, a integração com sistemas de gerenciamento de incidentes, a análise de tráfego e comportamento, testes de penetração, entre outras abordagens para aproveitar ao máximo os recursos que o Zabbix oferece e aprimorar ainda mais a segurança da infraestrutura de rede.

Além disso, seria interessante utilizar outros softwares de monitoramento em futuros trabalhos, tais como Nagios, Zenoss, OpenNMS, Dynatrace, Pandora FMS, entre outros, a fim de comparar os resultados.

Referências

ALENCAR, Márcio Aurélio dos Santos. *Fundamentos de Redes de Computadores*. Universidade Federal do Amazonas, CETAM, 2010. Citado 2 vezes nas páginas 21, 23.

BERNARDO, Cláudio. *Monitoramento de Redes com Zabbix*. 2018. Disponível em: https://claudiobernard0.wordpress.com/2018/01/25/monitoramento-de-redes-com-zabbix/. Acesso em: 23 jul. 2023. Citado 0 vez na página 36.

BERNERS-LEE, Tim. *Weaving the Web: the Original Design and Ultimate Destiny of the World Wide Web by Its Inventor*. New York: HarperCollins Publishers, 2000. Citado 1 vez na página 21.

CARLSSON, Thomas. Industrial network market shares 2023, mai. 2023. Disponível em: https://www.hms-networks.com/news-and-insights/news-from-hms/2023/05/05/industrial-network-market-shares-2023. Acesso em: 3 ago. 2023. Citado 0 vez na página 23.

CARTER, Roger. *Information Technology: Made Simple*. Elsevier Science, 2013. Citado 1 vez na página 18.

CISCO SYSTEMS, Inc. *Internetworking technologies handbook*. Cisco Press, 2004. Citado 1 vez na página 29.

DIAS, Beethovem Z; ALVES JR, Nilton. Protocolo de gerenciamento SNMP. *Nota Técnica CBPF-NT-006/01*, 2001. Acesso em: 5 jul. 2023. Citado 1 vez na página 29.

ELIAS, Glêdson; LOBATO, Luiz Carlos. *Arquitetura e Protocolo de Rede TCP-IP*. 2. ed. Rio de Janeiro: RNP/ESR, 2013. Citado 2 vezes nas páginas 25, 27, 28.

FIDLER, Bradley; CURRIE, Morgan. The Production and Interpretation of ARPANET Maps. *IEEE Annals of the History of Computing*, IEEE Computer Society, v. 37, n. 1, p. 44–55, 2015. Citado 0 vez na página 20.

FOROUZAN, Behrouz A. *Data Communications and Networking*. 5th ed.: McGraw Hill, 2013. Citado 1 vez nas páginas 23–25.

GALLOWAY, Brendan; HANCKE, Gerhard P. Introduction to industrial control networks. *IEEE Communications surveys & tutorials*, IEEE, v. 15, n. 2, p. 860–880, 2012. Citado 1 vez na página 22.

GONÇALVES, Felipe Antonio Machado Fagundes (Organizador). *Estudos Teórico-Metodológicos nas Ciências Exatas*. Ponta Grossa, PR: Atena, 2020. Citado 2 vezes na página 38.

GOYAL, Shivani. *Do You Know The Difference Between LAN, MAN, and WAN? Find Out Now!* 2022. unstop. Disponível em: https://unstop.com/blog/difference-between-lan-man-and-wan. Acesso em: 9 jul. 2023. Citado 0 vez na página 26.

HAFNER, Katie; LYON, Matthew. *Where Wizards Stay Up Late: The Origins of the Internet*. Simon & Schuster, 1998. Citado 1 vez na página 20.

HAUG, I. A.; HINTERHUBER, H. H. (Ed.). *Technological Operational Tools in the Manufacturing Sector: A Review of the State of the Art and Human Implications*. Springer, 2017. Citado 2 vezes na página 18.

HORST, Adail Spínola; SANTOS PIRES, Aécio dos; DÉO, André Luis Boni. *De A a Zabbix: Aprenda a monitorar e gerenciar aplicações e equipamentos de redes com o Zabbix*. Novatec Editora, 2015. Citado 2 vezes nas páginas 35, 37.

IBE, Oliver. *Converged Network Architectures: Delivering Voice and Data over IP, ATM, and Frame Relay*. Jan. 2001. ISBN 0471202509. Citado 1 vez na página 18.

IEC62443, ISA. *Security for Industrial Automation and Control Systems*. Geneva, CH, 2007-2018. Disponível em: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards. Acesso em: 16 jul. 2023. Citado 1 vez na página 31.

KUROSE, James F.; ROSS, Keith W. *Computer Networking: A Top-Down Approach*. Pearson, 2017. Citado 1 vez na página 21.

LAUDON, Kenneth C.; LAUDON, Jane P. *Sistemas de Informação Gerenciais*. Pearson, 2016. Citado 1 vez na página 17.

LEE, J.; BAGHERI, B.; KAO, H. A. A cyber-physical systems architecture for industry 4.0-based manufacturing systems. *Manufacturing letters*, v. 3, p. 18–23, 2015. Citado 2 vezes na página 18.

LONVICK, Chris M.; YLONEN, Tatu. *The Secure Shell (SSH) Protocol Architecture*. RFC Editor, jan. 2006. 30 p. RFC 4251. (Request for Comments, 4251). DOI: 10.17487/RFC4251. Disponível em: https://www.rfc-editor.org/info/rfc4251. Acesso em: 15 jul. 2023. Citado 1 vez na página 30.

LUGLI, Alexandre Baratella; SANTOS, Max Mauro Dias. *Redes industriais para automaçao industrial-As-I, Profibus e Profinet*. Saraiva Educação SA, 2010. Citado 1 vez na página 22.

MACEDO, Ricardo Tombesi et al. *Redes de Computadores*. Universidade Federal de Santa Maria. Núcleo de Tecnologia Educacional, 2018. Citado 9 vezes nas páginas 21, 27, 31–33.

MARSHALL, Perry S; RINALDI, John S. *Industrial Ethernet*. ISA, 2004. Citado 1 vez na página 28.

MONQUEIRO, Julio Cesar Bessa. *História das Redes de Computadores*. Abril 2008. Disponível em: https://www.hardware.com.br/tutoriais/historia-redes/. Acesso em: 3 mar. 2023. Citado 2 vezes nas páginas 19, 20.

OLUPS, Rihards. *Zabbix Network Monitoring*. Packt Publishing Ltd, 2016. Citado 2 vezes nas páginas 35, 36.

PATIL, Siddharth et al. *Predictive Maintenance Deloitte's Approach*. Deloitte Development LLC. 2022. Disponível em: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/process-and-operations/us-predictive-maintenance.pdf. Acesso em: 16 jul. 2023. Citado 1 vez na página 33.

PECENA, Wayne. *Is SNMP Really That Simple?* 2023. RADIOWORLD. Disponível em: https://www.radioworld.com/tech-and-gear/radio-it-management/is-snmp-really-that-simple. Acesso em: 10 jul. 2023. Citado 0 vez na página 30.

PEDRIALI, Diogo. *Convergência de TI e TO: Impactos na Segurança da Informação em Empresas com Manufatura Avançada*. 2021. Tese (Doutorado) – Centro Estadual de Educação Tecnológica Paula Souza, São Paulo. Disponível em: http://www.pos.cps.sp.gov.br/files/dissertacoes/file/341/91bd6bade178210ff1d769ae07cf79da.pdf. Acesso em: 23 abr. 2023. Citado 1 vez na página 18.

PEDRIALI, Diogo; GALEGALE, Napoleão Verardi; ARIMA, Carlos Hideo. Identificação da produção científica que aborda a convergência da tecnologia operacional com a tecnologia da informação. *Revista de Gestão e Secretariado (Management and Administrative Professional Review)*, v. 13, n. 4, p. 2374–2387, 2022. Citado 1 vez na página 19.

PETERSON, Larry L.; DAVIE, Bruce S. *Computer Networks: A Systems Approach*. Morgan Kaufmann, 2012. Citado 1 vez na página 21.

REIS LIMA, Janssen dos. *Monitoramento de Redes com Zabbix: Monitore a saúde dos servidores e equipamentos de redes*. Brasport, 2014. Citado 4 vezes nas páginas 35–37.

SENGUPTA, Jayasree; RUJ, Sushmita; DAS BIT, Sipra. A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT. *Journal of Network and Computer Applications*, v. 149, 2020. Disponível em: https://www.sciencedirect.com/science/article/pii/S1084804519303418. Acesso em: 24 jun. 2023. Citado 1 vez na página 19.

SIA, Zabbix. *ZABBIX Documentation*. 2021-2023. Disponível em: https://www.zabbix.com/documentation/5.0/en/manual. Acesso em: 25 jul. 2023. Citado 2 vezes nas páginas 37, 40.

SOUZA, Valdir Cardoso. *Organização e Gerência da Manutenção*. 5. ed. São Paulo: All Print, 2013. Citado 1 vez na página 33.

STALLINGS, William. *Network security essentials: Applications and standards, 4/e*. Pearson Education India, 2003. Citado 1 vez na página 31.

TANENBAUM, Andrew S.; WETHERALL, David J. *Computer Networks*. Pearson Education, 2010. Citado 2 vezes nas páginas 21, 22.

TONIDANDEL, Danny Augusto Vieira. Decifrando a transformada Z. In: CBA 2010 - XVIII Congresso Brasileiro de Automática. Set. 2010. Disponível em: http://bit.ly/2LJgKMv. Citado 1 vez na página 23.

TURBAN, Efraim; VOLONINO, Linda; WOOD, Gregory R. *Information Technology for Management: On-Demand Strategies for Performance, Growth, and Sustainability*. Wiley, 2015. Citado 1 vez na página 17.

WIZLYNX GROUP. *Avaliação de Segurança ICS*. 2023. wizlynx group. Disponível em: https://www.wizlynxgroup.com/br/seguranca-cibernetica-brasil/avaliacao-seguranca-ics. Acesso em: 17 jul. 2023. Citado 0 vez na página 29.