UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO
CENTRO DE CIÊNCIAS EXATAS, NATURAIS E DA SAÚDE
DEPARTAMENTO DE COMPUTAÇÃO

FÁBIO CIPRIANO SOAVE

ESTUDO COMPARATIVO DE FERRAMENTAS PARA GESTÃO DE CONFIGURAÇÕES DE REDES APLICADO AOS LABORATÓRIOS DE INFORMÁTICA DA UFES

ALEGRE - ES
2024

FÁBIO CIPRIANO SOAVE

ESTUDO COMPARATIVO DE FERRAMENTAS PARA GESTÃO DE CONFIGURAÇÕES DE REDES APLICADO AOS LABORATÓRIOS DE INFORMÁTICA DA UFES

Trabalho de Conclusão de Curso apresentado ao Departamento de Computação do Centro de Ciências Exatas, Naturais e da Saúde da Universidade Federal do Espírito Santo, como requisito parcial para obtenção do grau de Bacharel em Sistemas de Informação.
Orientador: Prof. Dr. Helder de Amorim Mendes

ALEGRE - ES
2024

Fábio Cipriano Soave

Estudo comparativo de ferramentas para gestão de configurações de redes aplicado aos laboratórios de informática da UFES

Trabalho de Conclusão de Curso apresentado ao Departamento de Computação do Centro de Ciências Exatas, Naturais e da Saúde da Universidade Federal do Espírito Santo, como requisito parcial para obtenção do grau de Bacharel em Sistemas de Informação.

Aprovado em 01 de outubro de 2024.

COMISSÃO EXAMINADORA

Prof. Dr. Helder de Amorim Mendes
Universidade Federal do Espírito Santo
Orientador

Prof. MSc. Giuliano Prado de Morais Giglio
Universidade Federal do Espírito Santo

Prof. Dr. Rodrigo Freitas Silva
Universidade Federal do Espírito Santo

AGRADECIMENTOS

Gostaria de expressar minha gratidão, primeiramente a Deus, por ter me guiado em todos os momentos ao longo desses anos de estudos. Agradeço também a Santo Antônio, cuja intercessão através das preces em cada trezena fortaleceu minha fé e meu caminho.

À minha família, pelo apoio incondicional, sem o qual nada disso seria possível.

Aos meus amigos, colegas e pelas experiências inesquecíveis vividas na Click Jr. e no movimento empresa júnior.

Aos amigos do grupo #*RU13hs*, que compartilharam muitos momentos comigo.

Um agradecimento especial ao Trailer Robson, cujos louvores pela manhã nos finais de período sempre trouxeram calma e alívio para enfrentar a reta final das disciplinas.

Por fim, sou profundamente grato aos professores e servidores com quem tive o privilégio de conviver e aprender durante todos esses anos.

“Pessoas são mais importantes que processos”
Adaptação, Manifesto Ágil (2001)

RESUMO

Pode-se afirmar que um laboratório de informática é dependente de uma infraestrutura confiável e segura, afim que o desempenho dos alunos não seja prejudicado por falhas de comunicação entre os dispositivos. Uma rede como essa está sujeita a atualizações de software e hardware seja pela atualização da tecnologia mantida pelo fabricante ou pela atualização da infraestrutura física. Passar por esse processo pode levar a um trabalho desgastante e oneroso, levando-se em conta, a quantidade de dispositivos impactados pela manutenção, o tamanho da rede, a disponibilidade de pessoal e do laboratório. Por isso, se faz necessário ter ferramentas que deem suporte a gestão dos laboratórios de informática tornando este procedimento mais ágil e automatizado, intervindo o mínimo possível na rotina dos laboratórios. Este trabalho visa avaliar qual ferramenta fornece uma solução para o gerenciamento de configurações da rede de Laboratórios de Informática da UFES - Campus Alegre, que atenda a demanda dos usuários e seja intuitiva para servidores e técnicos da UFES. Para essa avaliação, serão utilizadas métricas quantitativas e qualitativas para comparação entre as ferramentas, classificando-as entre si. Afim de que seja proposta uma ferramenta que satisfaça a realidade da rede dos laboratórios.

Palavras-chave: Gerenciamento de Redes, Ferramentas de Gerenciamento de Redes, Laboratório de Informática, Redes de Computadores.

ABSTRACT

It can be said that a computer laboratory depends on a reliable and secure infrastructure, so that student performance is not harmed by communication failures between devices. A network like this is subject to software and hardware updates, either by updating the technology maintained by the manufacturer or by updating the physical infrastructure. Going through this process can lead to exhausting and costly work, taking into account the number of devices impacted by maintenance, the size of the network, and the availability of personnel and the laboratory. Therefore, tools are needed to support the management of computer laboratories, making this procedure more agile and automated, intervening as little as possible in the laboratory routine. This work aims to evaluate which tool provides a solution for managing network configurations at the UFES Computer Laboratories - Campus Alegre, which meets user demand and is intuitive for UFES servers and technicians. For this evaluation, quantitative and qualitative analyzes will be used to compare the tools, classifying them among themselves. In order to propose a tool that meets the reality of the laboratory network.

Keywords: Network Management, Network Management Tools, Computer Laboratory, Computer Networks.

LISTA DE FIGURAS

Figura 01: Elementos da arquitetura de um sistema de gerência 21

Figura 02: Captura de tela do VirtualBox 29

Figura 03: Etapas do Projeto.....33

Figura 04: Configuração de download *Zabbix*.....37

Figura 05: Interface *web* configuração do *Zabbix*.....39

Figura 06: Interface inicial do *Zabbix*.....40

Figura 07: Configuração com o Banco de Dados.....40

Figura 08: Configurações finais.....41

Figura 09: Instalação concluída.....41

Figura 10: Tela de Login 42

Figura 11: Tela Principal 42

Figura 12: Lista de usuários no *Zabbix* 43

Figura 13: Configuração arquivo *zabbix_agentd.conf* 44

Figura 14: Agente *Zabbix* ativo.....44

Figura 15: *Hosts* monitorados 45

Figura 16: *E-mail* de alerta enviado.....46

Figura 17: Tela inicial do *Cacti* 51

Figura 18: Seleção de idioma *PRTG*.....54

Figura 19: Acordos de uso PRTG 55

Figura 20: Endereço de *e-mail PRTG* 55

Figura 21: Escolha método de instalação 56

Figura 22: Progresso instalação PRTG 56

Figura 23: Carregamento do PRTG 57

Figura 24: Tela de Login PRTG.....57

Figura 25: *Dashboard* PRTG.....58

Figura 26: Instalador *SolarWinds* 61

Figura 27: Método de instalação *SolarWinds* 62

Figura 28: Configuração da Instalação.....63

Figura 29: *Dashboard SolarWinds* 63

Figura 30: Laboratório de Desenvolvimento de *Software* 2.....71

Figura 31: Interface de monitoramento de *Hosts* 73

Figura 32: *Templates* do *Zabbix*.....74

Figura 33: Grupo de *hosts* do *Zabbix* 75

Figura 34: Relatórios programados 75

Figura 35: *Log* de auditoria 77

Figura 36: *Log* de ações.....78

Figura 37: *Scripts* personalizáveis.....79

Figura 38: Menu de Alertas 80

Figura 39: Menu de Alertas 81

Figura 40: *Templates* do *Zabbix*.....81

Figura 41: Mapas de redes do *Zabbix*.....83

Figura 42: Resumo detalhado do *Host* 85

Figura 43: Mapa de rede 86

Figura 44: Tela de configuração de alertas 87

Figura 45: *IPs* de cada interface do LAB06-08 88

Figura 46: *Descoberta de rede* 89

LISTA DE TABELAS

Tabela 1 - Método de avaliação 34

Tabela 2 - Comparação.....36

Tabela 3 - Resultados Comparativo Teste Virtual 68

LISTA DE ABREVIATURAS E SIGLAS

CPU – Central Processing Unit

CMIP – Common Management Information Protocol

FCAPS – Fault, Configuration, Accounting, Performance and Security

ICMP – Internet Control Message Protocol

MIB – Management Information Base

OSI – Open System Interconnection

QoS – Quality of Service

SNMP – Simple Network Management Protocol

TCP/IP – Transmission Control Protocol/Internet Protocol

UFES – Universidade Federal do Espírito Santo

WAN – Wide Area Network

SUMÁRIO

1. INTRODUÇÃO 15

1.1. O PROBLEMA E SUA IMPORTÂNCIA 15

1.2. OBJETIVOS 17

1.2.1. OBJETIVO GERAL 17

1.2.2. OBJETIVOS ESPECÍFICOS 17

1.3. ESTRUTURA DO TRABALHO 17

2. REVISÃO DA LITERATURA 18

2.1. GERENCIAMENTO DE REDES 18

2.2. FERRAMENTAS DE GERENCIAMENTO DE REDES 25

2.2.1. ZABBIX 25

2.2.2. CACTI 26

2.2.3. PRTG NETWORK MONITOR 26

2.2.4. SOLARWINDS 27

2.3. SNMP 27

2.4. CONFIGURAÇÃO DO VIRTUALBOX 28

2.5. CRITÉRIOS DE AVALIAÇÃO 30

2.5.1. AVALIAÇÃO 30

2.5.2. MÉTRICAS 31

3. METODOLOGIA 33

4. RESULTADOS E DISCUSSÃO 37

4.1. TESTE VIRTUAL 37

4.2. TESTE VIRTUAL: ZABBIX 37

4.2.1. PROCEDIMENTOS EXECUTADOS: ZABBIX 46

4.2.2. COMPORTAMENTOS OBSERVADOS: ZABBIX 48

4.3. TESTE VIRTUAL: CACTI 49

4.3.1. PROCEDIMENTOS EXECUTADOS: CACTI 52

4.3.2. COMPORTAMENTOS OBSERVADOS: CACTI 53

4.4. TESTE VIRTUAL: PRTG NETWORK MONITOR 54

4.4.1. PROCEDIMENTOS EXECUTADOS: PRTG NETWORK MONITOR 58

4.4.2. COMPORTAMENTOS OBSERVADOS: PRTG NETWORK MONITOR 60

4.5. TESTE VIRTUAL: SOLARWINDS 61

4.5.1. PROCEDIMENTOS EXECUTADOS: SOLARWINDS 64

4.5.2. COMPORTAMENTOS OBSERVADOS: SOLARWINDS 66

4.6. RESULTADOS DO TESTE VIRTUAL 67

4.7. TESTE FÍSICO 70

4.7.1. PREPARAÇÃO DO AMBIENTE 70

4.7.2. TESTE FÍSICO: ZABBIX 72

4.7.3. TESTE FÍSICO: SOLARWINDS 84

5. CONCLUSÃO 90

REFERÊNCIAS 92

1. INTRODUÇÃO

Com o avanço das tecnologias e o crescente volume de dados que circulam pelas redes de computadores, torna-se imprescindível a adoção de soluções tecnológicas que garantam a confiabilidade, interoperabilidade, redundância e segurança tanto para os usuários quanto para os dados trafegados nessas redes. O gerenciamento de redes, por sua vez, desempenha um papel crucial na manutenção da confiabilidade, escalabilidade e administração dessas infraestruturas, assegurando o funcionamento eficiente e seguro das comunicações digitais.

As redes de computadores estão em constante evolução, incorporando componentes de diferentes fornecedores e configurações. Mesmo as redes mais simples exigem gerenciamento adequado para garantir a disponibilidade dos serviços de maneira satisfatória para os usuários (BLACK, 2008). No entanto, gerenciar essas redes manualmente, dispositivo por dispositivo, torna-se cada vez mais inviável, especialmente considerando a complexidade crescente dessas infraestruturas. Para enfrentar esse desafio, surgiram *softwares* de gerenciamento de redes que otimizam os processos de manutenção e melhoria, oferecendo uma ampla gama de configurações, monitoramento de dados em tempo real e compatibilidade com diversos dispositivos e sistemas.

Um laboratório de informática precisa estar sempre disponível, funcional e operante em sua capacidade máxima, de modo a não causar impactos negativos nas atividades pedagógicas e de pesquisa dos usuários. Nesse sentido, contar com o apoio de um software de gestão de rede torna-se cada vez mais indispensável e vantajoso.

1.1. O PROBLEMA E SUA IMPORTÂNCIA

Para Macedo *Et al* (2018) “o gerenciamento de redes trata de uma área fundamental relacionada as redes de computadores, pois objetiva o controle das atividades e o monitoramento do uso de recursos no ambiente de redes.” As atuais redes, são formadas por vários tipos de componentes diferentes que precisam se comunicar e trocar informações sejam para o próprio funcionamento ou pela solicitação dos usuários. Para que isso ocorra com eficiência, é preciso que todo esse sistema tenha

um bom desempenho. E para alcançar essa eficiência se faz necessário ter ferramentas que auxiliem o gestor da rede com o seu gerenciamento.

Segundo Moura (2005), o gerenciamento de redes pode ser entendido como o “acompanhamento dos eventos de uma rede, a fim de diagnosticar problemas e determinar quando e quais procedimentos de contingência devem ser aplicados, bem como obter estatísticas para administração e optimização de desempenho.” Stallings (1999) complementa quando afirma que os softwares de gestão de redes auxiliam na tarefa de gerenciar as redes, coletando informações dos componentes e otimizando as atividades da gerência.

De acordo com Boutaba e Polyrakis (2001), definem gerência de configuração como sendo os parâmetros de funcionamento da rede através de alterações de sua configuração atendendo as mudanças de infraestrutura e alcançando critérios de Qualidade do Serviço (QoS). Para Goyal, Mikkilineni e Ganti (2009) a gerência de configuração envolve tarefas de alto nível, a falha ou indisponibilidade de algum serviço causa um grande impacto negativo em toda a rede. É responsabilidade, também, da gestão de configuração manter informações sobre as configurações dos dispositivos afim de estabelecer uma base histórica que inicialize ou encerre serviços de maneira correta. (Gorod; Sauser; Boardman, 2008).

Observa-se que a correta gestão de configuração é a base para a operação com eficácia e a eficiência dos serviços como um todo. Incidindo que a execução de manutenções na topologia através da configuração de vários dispositivos e a análise do impacto destas alterações no ambiente são práticas fundamentais da gerência de configuração. (TERAMOTO et al., 2013).

Compreendendo que um laboratório de informática precisa estar operante para o seu uso e que situações adversas podem acontecer como a falha de equipamentos, atualizações de *hardwares* ou atualizações tecnológicas. Juntamente com as citações referenciadas acima, pode-se concluir que é fundamental ter uma ferramenta de gestão de configuração para a rede de Laboratórios de informática da UFES Campus Alegre. Devido a isso, definir qual ferramenta que se adaptará melhor a este cenário e as condições avaliadas é o objeto de estudo deste trabalho.

1.2. OBJETIVOS

1.2.1. OBJETIVO GERAL

O propósito principal deste estudo é realizar uma comparação entre as ferramentas de Gerenciamento de Configuração de Redes disponíveis atualmente no mercado, com o intuito de avaliar sua viabilidade para utilização nos Laboratórios de Informática da UFES - Campus Alegre.

1.2.2. OBJETIVOS ESPECÍFICOS

a) Realizar um estudo das ferramentas de Gerenciamento de Configuração de Rede, com o objetivo de analisar sua aplicabilidade na rede dos Laboratórios de Informática;
b) Implementar as ferramentas em um ambiente controlado, conduzindo uma classificação baseada em métricas quantitativas e qualitativas;
c) Avaliar os resultados obtidos e propor a ferramenta mais adequada para ser utilizada nos Laboratórios de Informática da UFES - Campus Alegre.

1.3. ESTRUTURA DO TRABALHO

Este estudo está organizado da seguinte maneira: no segundo capítulo, é realizada uma revisão geral sobre redes de computadores, abordando o gerenciamento de rede e as ferramentas de configuração utilizadas. No terceiro capítulo, é apresentada a metodologia de pesquisa empregada. Finalmente, no quarto capítulo, são discutidos os resultados obtidos durante a aplicação da metodologia.

2. REVISÃO DA LITERATURA

Este capítulo apresenta uma revisão da literatura relevante ao tema de redes de computadores e gerenciamento de rede, com foco nas ferramentas de configuração de redes. Inicialmente, será abordada a evolução das redes de computadores e sua importância no contexto atual, seguido por uma análise das práticas de gerenciamento de redes. Em seguida, será discutido o papel das ferramentas de configuração de redes na otimização da administração e manutenção dos ambientes de rede, destacando as principais características e funcionalidades das soluções mais utilizadas no mercado. Esta revisão tem como objetivo fundamentar teoricamente a pesquisa, proporcionando uma compreensão abrangente dos conceitos e tecnologias que serão explorados nos capítulos subsequentes.

2.1. GERENCIAMENTO DE REDES

As redes de computadores são sistemas interconectados que permitem a troca de informações e recursos entre diferentes dispositivos. Elas têm sido essenciais para a comunicação e o compartilhamento de dados em escala global. Ao longo dos anos, as redes de computadores evoluíram significativamente, tanto em termos de tamanho quanto de complexidade.

No passado, as redes de computadores eram mais limitadas em alcance e capacidade. Elas eram predominantemente utilizadas em ambientes corporativos e acadêmicos, interligando computadores individuais em uma área geograficamente restrita. Essas redes eram geralmente baseadas em tecnologias como *Ethernet* e protocolo *TCP/IP*.

A evolução das redes de computadores possibilitou a criação de redes de maior escala, como redes de área ampla (WAN) que interligam diferentes locais geográficos, e a Internet, que conecta redes em todo o mundo. Além disso, as velocidades de transmissão de dados aumentaram consideravelmente, permitindo transferências de arquivos mais rápidas e comunicação em tempo real.

O aumento do número de dispositivos conectados trouxe benefícios e desafios. Por um lado, a conectividade em larga escala facilitou a colaboração, o acesso à informação e o compartilhamento de recursos. Por outro lado, a segurança e a privacidade se tornaram preocupações significativas, pois mais dispositivos estão expostos a ameaças cibernéticas.

A administração e o gerenciamento de redes se tornaram mais complexos, exigindo soluções de gerenciamento de configuração, monitoramento e manutenção eficientes. Em suma, as redes de computadores evoluíram para atender às necessidades de uma sociedade cada vez mais conectada. O aumento do número de dispositivos conectados proporcionou maior acessibilidade e comunicação, mas também exigiu uma abordagem cuidadosa em relação à segurança e ao gerenciamento das redes.

Independentemente do tamanho de uma rede de computadores, é essencial que ela seja gerenciada e controlada. O gerenciamento de redes de computadores envolve lidar com possíveis falhas, inoperâncias não previstas ou comportamentos inconsistentes. Quando tais eventos ocorrem, o administrador de rede deve estar preparado para mitigar os impactos negativos dessas situações. Essa ação pode ser realizada de forma automatizada por meio de um software ou com base em documentação pré-estabelecida (Bieszcad et al., 1998). É fundamental que o sistema funcione de maneira adequada e não cause prejuízos aos usuários. Para que o administrador de redes possa desempenhar suas atividades com qualidade, é essencial contar com softwares que o auxiliem no controle operacional completo.

Forouzan e Mosharraf (2013) definem gerenciamento de redes como a ação “de testar, monitorar, configurar e resolver problemas dos componentes de rede com o objetivo de atender um conjunto de requisitos definidos por uma organização”. Ou seja, gerenciar uma rede é garantir um certo nível de qualidade dos serviços por ela ofertada por meio de monitoramento e controle dos seus recursos.

Conforme descrito por Lopes, Sauvé e Nicoletti (2002), um sistema de gerenciamento é composto por quatro componentes básicos conforme apresentado na Figura 1:

- **Elementos gerenciados:** Esses componentes referem-se aos equipamentos que estão sendo monitorados pela estação de gerenciamento. Isso inclui

roteadores, switches, servidores, dispositivos de armazenamento e outros dispositivos de rede que são alvo do processo de gerenciamento.

- **Estação de gerência:** Essa é a central de operações do gerenciamento de redes, onde os usuários podem monitorar e controlar todo o sistema. A estação de gerenciamento fornece uma interface para visualizar informações, gerar relatórios, configurar dispositivos e realizar outras tarefas relacionadas ao gerenciamento da rede.
- **Protocolo de gerência:** Trata-se do protocolo utilizado para a comunicação entre as estações gerenciadas (elementos gerenciados) e a estação de gerenciamento. Esse protocolo define as regras e formatos de mensagem para a transmissão de informações entre os componentes do sistema de gerenciamento. Exemplos de protocolos de gerenciamento incluem o SNMP (*Simple Network Management Protocol*) e o CMIP (*Common Management Information Protocol*).
- **Informações de gerência**: São os dados que trafegam entre os elementos gerenciados e a estação de gerenciamento por meio do protocolo de gerenciamento. Essas informações podem incluir dados de desempenho, status de dispositivos, registros de eventos, configurações e outras informações relevantes para o gerenciamento da rede. Esses dados permitem que os administradores monitorem o estado da rede, tomem decisões baseadas em informações atualizadas e realizem ações corretivas quando necessário.

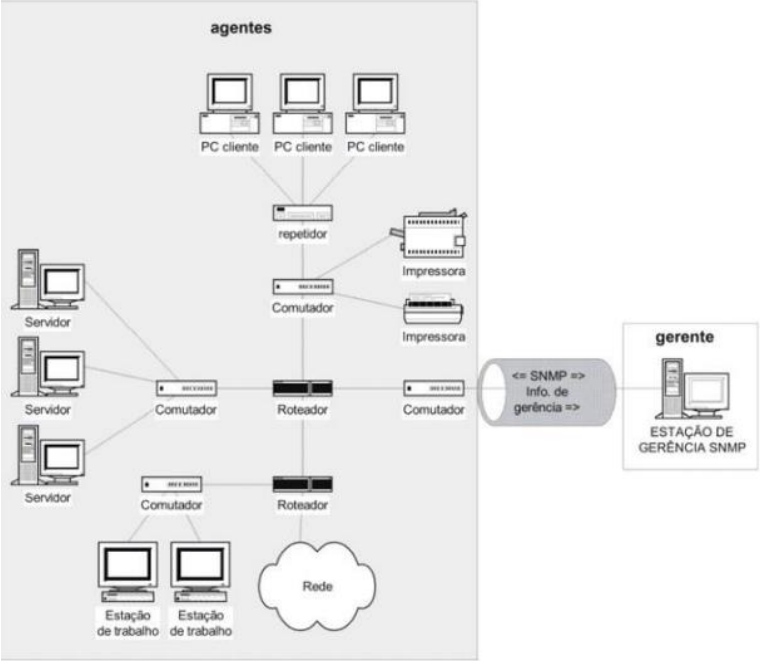
A Figura 01 ilustra os elementos da arquitetura de um sistema de gerência de rede, destacando a interação entre os componentes distribuídos em uma infraestrutura de TI.

A arquitetura é composta por dois principais blocos: agentes e o gerente. O bloco de agentes representa os dispositivos e sistemas da rede, como servidores, *PCs* clientes, estações de trabalho, roteadores, comutadores, e impressoras, que interagem entre si através de diversos dispositivos intermediários, como repetidores, comutadores e roteadores. Estes agentes são responsáveis por fornecer informações sobre seu status e desempenho ao sistema de gerência.

No centro da imagem, há uma rede conectada por roteadores e comutadores, que facilitam a comunicação entre os diferentes agentes da rede. Cada um desses agentes está vinculado a um protocolo *SNMP (Simple Network Management Protocol)*, que coleta e transfere informações de gerência, como status operacional e dados de desempenho, para a estação de gerência *SNMP*.

O bloco do gerente é representado pela estação de gerência *SNMP*, que centraliza a coleta e análise dos dados recebidos dos agentes distribuídos. Esta estação é o ponto de controle que permite monitorar e gerenciar o estado de todos os dispositivos da rede de forma eficiente, facilitando a tomada de decisões de administração e correção de problemas.

Figura 01: Elementos da arquitetura de um sistema de gerência



Fonte: Lopes, Sauvé e Nicoletti (2002)

Essa arquitetura reflete a importância de uma estrutura de gerência eficiente, que garante a interoperabilidade e supervisão dos elementos críticos em redes complexas, assegurando o funcionamento adequado dos recursos de TI. Segundo Lopes, Sauvé e Nicoletti (2002), essa configuração é fundamental para a manutenção e operação de redes em um contexto corporativo, permitindo a identificação e resolução de falhas de forma proativa.

De acordo com a ISO 7498-4, a gerência de redes é dividida em cinco áreas funcionais distintas: gerenciamento de falhas, gerenciamento de configuração, gerenciamento

de contabilização, gerenciamento de desempenho e gerenciamento de segurança. Essa classificação é comumente representada pelo acrônimo FCAPS (*Fault, Configuration, Accounting, Performance and Security*), que foi desenvolvido para o modelo OSI. Como resultado, fabricantes de hardware e software de redes adotaram essa padronização em suas tecnologias.

Para Eler (2015), o gerenciamento de falhas pode ser definido como a "função de monitorar os estados dos recursos verificando em qual ponto da rede e quando uma falha ou um erro pode ocorrer". Falhas não são o mesmo que erros. Andreoli (2016), discute a diferença entre a falha e o erro,

> "uma falha é uma condição anormal persistente e que causa a total interrupção da rede, como, por exemplo, o rompimento de um cabo; uma falha exige uma ação de gerenciamento imediata. Um erro é uma condição anormal ocasional que pode ser corrigida ou compensada antes que se transforme em uma falha, tendo como exemplo, erro de bits durante uma transmissão."

Segundo Filho (2012), a gerência de falhas possui três grandes responsabilidades: "o monitoramento dos estados dos recursos da rede, a manutenção de cada um dos objetos gerenciados e as decisões que devem ser tomadas para restabelecer as unidades do sistema que possam apresentar problemas". É ideal que se saiba as falhas que podem ocorrer antes que elas aconteçam.

Forouzan (2007), destaca quatro atribuições para o gerenciamento de falhas. O primeiro é sobre detectar o local onde a falha ocorreu, o segundo, trata sobre isolar a falha do restante da rede, o que diminui significativamente o impacto causado. Após detectar e isolar, é preciso fazer a correção da falha, que é a matéria de estudo da gerência de falhas e por fim, documentar a falha, elaborando uma documentação detalhada sobre o ocorrido a fim de montar uma biblioteca com todas as falhas ocorridas e as soluções tomadas, assim para que no futuro quando volte a acontecer o processo de reparo seja mais ágil.

Para Junior (2012), o gerenciamento de desempenho "é um conjunto de funções responsáveis por garantirem que não ocorram insuficiências de recursos quando sua utilização se aproximar da capacidade total do sistema". Ou seja, a gerência de

desempenho preocupa-se com a performance da rede, se ela é eficiente e se atende aos parâmetros esperados.

A gerência de contabilidade como o próprio nome diz, se trata dos recursos contábeis da rede. Recursos esses pagos em dinheiro para o seu uso. Por isso Kock (1997) define ser vital definir “os custos e volumes de recursos utilizados pelos usuários sejam identificados e registrados de forma correta.”

Para Clara (1993) a gerência de segurança tem como “objetivo criar, controlar e eliminar mecanismos de segurança bem como distribuir informações relevantes à segurança, gerando alarmes para o gerente da rede quando for detectado algum evento de segurança”. A gerência de segurança trata sobre a geração, controle e distribuição de chaves de criptografia, o controle de acesso a rede, monitoria dos agentes além de realizar exames de auditoria e armazenagem de logs de segurança, Em resumo, é responsável por “proteger os recursos da rede e as informações dos usuários”. (Filho, 2012).

Uma rede de computadores, está em constante evolução, novos equipamentos são inseridos, ou substituídos por falhas, ou pela atualização de hardware da infraestrutura. Para Eler (2015), o gerenciamento de configuração “permite manter atualizadas as informações de hardware e software de uma rede, incluindo as informações de configurações de todos os equipamentos”. Filho (2012), complementa que “também está relacionado às tarefas de manutenção, adição e atualização de relacionamentos entre os componentes e da situação dos componentes durante a operação da rede.

O gerenciamento de configurações tem como responsabilidade manter as configurações de dispositivos, registrar alterações nessas configurações, identificar os dispositivos e componentes, além de realizar ações que causem o menor impacto possível na rede, visando minimizar falhas ou indisponibilidades dos serviços. Dadas essas mudanças constantes e a necessidade de mentar em plena operação, ou seja, sem interrupção dos serviços, podemos afirmar que é vital ter um processo definido de gerência de configuração de redes. (Vanz, 2016).

Forouzan (2010) organiza o gerenciamento de configuração em duas frentes:

- **Reconfiguração:** atende as alterações de hardware, sendo elas físicas como substituição ou implementação de novos equipamentos ou logica devido a mudanças de topologia ou para atender a uma nova configuração da rede.
- **Documentação:** como o próprio nome diz, é o registro de cada alteração dos hardwares ou softwares presentes na rede. Pode ser realizado por diagramas com localização física dos dispositivos bem como a apresentação das configurações estabelecidas para cada dispositivo no cenário da rede. Cabe também, manter especificações técnicas dos dispositivos, o que contribui para o gerenciamento de contabilidade.

O gerenciamento de configuração é uma das áreas funcionais essenciais no campo de gerenciamento de redes. Ele abrange processos e práticas que visam controlar e monitorar as configurações dos dispositivos e componentes de uma rede. O objetivo do gerenciamento de configuração é garantir que as configurações sejam consistentes, corretas e alinhadas com as necessidades e políticas estabelecidas. Isso facilita a manutenção, o controle de mudanças e a solução de problemas na rede, além de contribuir para a estabilidade, segurança e eficiência operacional do ambiente de rede como um todo.

É importante ressaltar que este trabalho tem como foco as ferramentas específicas de gerenciamento de configuração para a rede de computadores dos laboratórios de informática. O objetivo é avaliar e comparar as opções disponíveis no mercado, levando em consideração as necessidades e requisitos específicos desses laboratórios.

O gerenciamento de configuração desempenha um papel fundamental na garantia da estabilidade, integridade e eficiência da rede, além de facilitar a manutenção e o controle de mudanças. Portanto, a escolha adequada de uma ferramenta de gerenciamento de configuração é essencial para assegurar o bom funcionamento dos laboratórios de informática e atender às demandas dos usuários de forma eficaz.

2.2. FERRAMENTAS DE GERENCIAMENTO DE REDES

A seguir, são apresentadas as ferramentas que são objeto de estudo neste trabalho, juntamente com uma breve descrição de suas características que podem trazer benefícios para o gerenciamento de configuração de redes nos Laboratórios de Informática da UFES. As ferramentas selecionadas para este estudo foram escolhidas com base em uma busca no Google e foi selecionado os 4 primeiros resultados retornados pelo buscador.

2.2.1. ZABBIX

O *Zabbix* é uma ferramenta que aborda várias áreas do gerenciamento de redes, tendo sido projetada para monitorar a disponibilidade, a experiência do usuário e a qualidade dos serviços. O *Zabbix* é uma solução de código aberto e gratuita, conhecida por sua flexibilidade e por oferecer uma ampla gama de recursos. A ferramenta é constantemente atualizada e conta com uma comunidade ativa de usuários e desenvolvedores. Uma das vantagens do *Zabbix* é sua capacidade de integração com diversos sistemas operacionais e dispositivos de rede, permitindo monitorar uma ampla variedade de componentes em um ambiente heterogêneo. A gestão do *Zabbix* é realizada por meio de uma interface web amigável, facilitando a configuração e o gerenciamento da ferramenta. (ZABBIX, 2023).

Além disso, o *Zabbix* oferece suporte à integração com bancos de dados e a execução de scripts personalizados, permitindo a adaptação da ferramenta às necessidades específicas do ambiente de rede. Isso possibilita a personalização e à automação de tarefas de gerenciamento. (ZABBIX, 2023).

Com seu conjunto de recursos abrangentes, o *Zabbix* permite o monitoramento de diversos aspectos da rede, como disponibilidade de dispositivos, desempenho, tráfego, eventos e até mesmo a experiência do usuário. Essas informações são apresentadas por meio de gráficos, alertas e relatórios, auxiliando os administradores na identificação e solução de problemas de forma eficiente.

Em resumo, o *Zabbix* é uma ferramenta personalizável em diversas configurações oferecendo recursos abrangentes para o gerenciamento de redes. Sua natureza *open-*

source, integrações e suporte a sistemas operacionais diversos tornam-no uma escolha popular para organizações que desejam um monitoramento eficaz e personalizado de sua infraestrutura de rede. (Zabbix, 2023).

2.2.2. CACTI

Segundo o CACTI (2021) é uma ferramenta de monitoramento de rede inicialmente desenvolvida para monitorar o desempenho da rede. No entanto, por meio do uso de plugins, sua funcionalidade foi expandida para abranger uma ampla variedade de recursos, como gerenciamento de falhas, segurança e configuração. Essa capacidade de expansão é um dos principais pontos fortes do *CACTI*.

Sendo uma ferramenta *open-source*, o *CACTI* permite que os usuários personalizem e estendam suas funcionalidades de acordo com suas necessidades específicas. Além disso, oferece recursos para gestão de usuários, permitindo controlar o acesso e as permissões dos usuários do sistema. Adicionalmente, suporta a execução de scripts personalizados, possibilitando a automação de tarefas específicas.

O *CACTI* é uma solução comumente adotada por administradores de redes para monitoramento de redes, fornecendo uma interface amigável e recursos versáteis.

2.2.3. PRTG NETWORK MONITOR

O *PRTG* é uma ferramenta de gerenciamento de redes que é instalada em um servidor e pode ser acessada por meio de uma interface *web* ou aplicativo nativo. Ele oferece recursos abrangentes de monitoramento de sistemas, dispositivos, aplicativos, tráfego e outros elementos da rede. O *PRTG* é um software proprietário, mas também possui uma versão gratuita que permite até 100 sensores, o que pode ser suficiente para atender às necessidades de experimentação neste estudo. (PAESSLER IOT, 2023)

Uma das características distintivas do *PRTG* é a sua licença perpétua, o que significa que não há necessidade de renovação anual ou pagamento de taxas recorrentes. Além disso, o *PRTG* oferece recursos avançados, como descoberta automática de dispositivos na rede, permitindo uma fácil configuração e monitoramento de novos dispositivos. Ele também oferece uma ampla gama de recursos personalizados e

completos para atender às necessidades específicas de gerenciamento de rede. (PAESSLER IOT, 2023).

2.2.4. SOLARWINDS

Segundo SOLARWINDS (2023) se trata uma solução abrangente de gerenciamento de redes que vai além da gestão de configuração, oferecendo recursos de monitoramento de segurança, desempenho e gestão de falhas. Uma de suas funcionalidades é o localizador de dispositivos, que permite mapear e fazer um inventário de toda a rede de forma rápida e fácil.

A interface do *SolarWinds* é conhecida por sua aparência limpa e intuitiva, oferecendo uma ampla gama de dados monitorados para uma visão abrangente da rede. No que diz respeito à gestão de configuração, o software oferece recursos de automação, como *backups* de configurações, rastreamento de alterações e proteção contra alterações não planejadas por meio de fluxos de trabalho. (SOLARWINDS, 2023)

O *SolarWinds* também realiza auditoria da rede e detecta possíveis vulnerabilidades, proporcionando uma camada adicional de segurança. Além disso, a ferramenta facilita a configuração de *switches*, roteadores e rotas, simplificando o processo de gerenciamento da infraestrutura de rede.

Como um *software* de gerenciamento de redes completo, o *SolarWinds* oferece uma ampla gama de recursos para garantir o desempenho, a segurança e a confiabilidade da rede. Com suas capacidades abrangentes, ele atende às necessidades de gestão de configuração, bem como a outras áreas críticas de gerenciamento de redes. (SOLARWINDS, 2023).

2.3. SNMP

O protocolo *Simple Network Management Protocol* (SNMP) é um protocolo amplamente utilizado para gerenciamento e monitoramento de dispositivos em redes

de computadores. Ele foi desenvolvido para facilitar a coleta de informações e o controle de dispositivos de rede, como roteadores, *switches* e servidores.

O SNMP funciona através de uma arquitetura cliente-servidor, onde os dispositivos de rede atuam como agentes SNMP e são monitorados por uma estação de gerenciamento SNMP. O protocolo permite que a estação de gerenciamento solicite informações dos agentes, como dados de desempenho, status de conexão e eventos do sistema. Além disso, o SNMP também permite o envio de comandos de controle para configurar e modificar o comportamento dos dispositivos gerenciados.

O SNMP utiliza uma estrutura de gerenciamento baseada em MIB (*Management Information Base*), que define as informações e parâmetros disponíveis para monitoramento e controle. Através das MIBs, é possível acessar informações específicas de cada dispositivo e realizar ações de gerenciamento de forma padronizada.

Em resumo, o SNMP desempenha um papel fundamental no gerenciamento de redes, permitindo o monitoramento proativo, a detecção de falhas, a análise de desempenho e a configuração de dispositivos de rede. Sua flexibilidade e interoperabilidade o tornaram um dos protocolos mais utilizados na indústria de redes, fornecendo uma base sólida para o gerenciamento eficiente de redes de computadores.

2.4. CONFIGURAÇÃO DO VIRTUALBOX

O *VirtualBox* é um *software* de virtualização de código aberto desenvolvido pela *Oracle Corporation*. Essa plataforma permite a criação e execução de máquinas virtuais em diversos sistemas operacionais, proporcionando um ambiente isolado para testes, desenvolvimento e experimentação. (VIRTUALBOX, 2023)

Com suporte para uma variedade de sistemas operacionais, incluindo *Windows*, *Linux*, *macOS* e outros, o *VirtualBox* oferece flexibilidade para os usuários explorarem diferentes ambientes de *software* sem a necessidade de instalação direta em seus sistemas físicos.

O *VirtualBox* foi empregado para conduzir os testes virtuais neste trabalho, envolvendo três servidores *Linux Ubuntu* e um ambiente de trabalho *Ubuntu*. A

escolha de apenas quatro máquinas virtuais foi determinada por limitações técnicas associadas à capacidade operacional do computador utilizado para a realização dos testes. Cada máquina foi configurada para consumir o mínimo de recursos computacionais possível, otimizando assim o desempenho do ambiente virtual. A captura de tela do *VirtualBox* em execução, apresentada na Figura 02 abaixo, destaca a configuração das máquinas virtuais, proporcionando uma visão visual do ambiente de teste.

Figura 02: Captura de tela do VirtualBox

Fonte: Autor

Foram realizadas verificações para confirmar se as máquinas estavam estabelecendo conexão com o computador hospedeiro e se respondiam aos comandos de *ping*.

2.5. CRITÉRIOS DE AVALIAÇÃO

Nesta seção, serão apresentados os critérios utilizados para avaliar e distinguir os softwares de gerenciamento de redes que foram analisados neste trabalho.

2.5.1. AVALIAÇÃO

As ferramentas serão estudadas separadamente, ou seja, cada ferramenta será analisada e implantada isoladamente, sem que uma interfira na execução da outra. Entende-se que a ferramenta que melhor atenda os critérios é a que terá o resultado mais satisfatório em operação nos Laboratórios de Informática. As ferramentas serão avaliadas em 5 pontos macros com o objetivo mais amplo:

- **Funcionalidades:** Esse critério avaliará as funcionalidades oferecidas por cada software, como automação de configuração, detecção de falhas, geração de relatórios, programação automatizada, entre outros. Será levado em consideração o conjunto de recursos que cada ferramenta disponibiliza para o gerenciamento de configuração de redes.
- **Usabilidade:** Será analisada a facilidade de uso e a interface do software. Critérios como intuitividade, clareza na apresentação das informações e facilidade na realização das tarefas serão considerados. Um software com uma interface amigável e intuitiva tende a facilitar o trabalho do administrador de rede.
- **Escalabilidade:** Esse critério avaliará a capacidade do software de gerenciar redes em diferentes tamanhos e complexidades. Será analisado se o software é capaz de lidar com redes de pequeno, médio e grande porte, considerando a capacidade de gerenciamento centralizado e distribuído.
- **Integração:** Será verificado se o software possui recursos de integração com outros sistemas e dispositivos de rede. A capacidade de integração com equipamentos de diferentes fabricantes e a interoperabilidade com outros softwares de gerenciamento serão levadas em consideração.
- **Suporte e documentação:** Será avaliada a disponibilidade de suporte técnico oferecido pelo fabricante do software, bem como a qualidade da documentação disponível. Um bom suporte e documentação adequada são importantes para

auxiliar o administrador de rede em possíveis dúvidas ou problemas que possam surgir durante o uso do software.

Esses critérios serão utilizados como base para a análise comparativa dos softwares de gerenciamento de redes, visando identificar as características distintas de cada ferramenta e determinar qual delas é mais adequada para atender às necessidades de gerenciamento de configuração de redes dos Laboratórios de Informática da UFES.

2.5.2. MÉTRICAS

A ISO/IEC/IEEE 24765, 2010 estabelece que "métrica" é uma medida utilizada para avaliar se um sistema, componente ou processo possui determinado atributo. Para a avaliação de um software, é necessário ter clareza nos critérios avaliados, bem como definir métricas específicas para cada um deles. É importante evitar questões abertas ou ambíguas que possam levar a interpretações que distorçam o resultado final. Métricas objetivas não levam em consideração o ponto de vista de quem as interpreta, focando apenas no objetivo a ser analisado (SATO, 2007). Isso contribui para obter resultados concisos e precisos.

No ponto de avaliação da implementação dos softwares, será analisada a facilidade de instalação das ferramentas, não a configuração dos equipamentos.

- **Grau de dificuldade da instalação:** essa métrica avalia o nível de dificuldade para a instalação dos softwares, se a documentação fornece informações suficientes para a instalação bem-sucedida ou se é necessário recorrer à internet para concluir o processo, além de verificar se são necessárias liberações ou configurações de outros serviços para o pleno funcionamento da ferramenta.
- **Tempo:** essa métrica visa medir o tempo total necessário para a instalação dos softwares, desde o início do download até a conclusão da instalação, incluindo a resolução de eventuais problemas durante o processo, até que a ferramenta possa ser acessada sem erros.

Na avaliação da configuração, será mensurada a forma como os dispositivos na rede são configurados.

- **Descoberta automática de dispositivos:** essa métrica avalia se as ferramentas têm a capacidade de realizar automaticamente a descoberta dos dispositivos na rede.
- **Configuração:** avalia como cada ferramenta se comporta na implementação das regras e características necessárias para cada dispositivo ao ser inserido na rede.
- **Grau de dificuldade:** de forma semelhante à métrica de implementação, busca-se medir a dificuldade encontrada, os problemas enfrentados e a capacidade de resolvê-los utilizando a documentação de instalação, ou quando é necessário recorrer a fontes externas à documentação.

No penúltimo ponto de avaliação deste trabalho, é considerada a clareza de todas as operações do sistema, ou seja, a facilidade de compreensão das informações para aqueles que trabalham diariamente com as ferramentas.

- **Interface gráfica:** esse é um recurso importante que facilita a usabilidade do administrador do sistema e agiliza suas tarefas.
- **Nível de acesso à informação:** refere-se à forma como as informações são apresentadas e à facilidade de operação do sistema. Isso inclui a qualidade das informações, de modo que o administrador seja capaz de interpretá-las no momento em que são apresentadas, sem a necessidade de buscar no contexto da documentação ou fora dela.

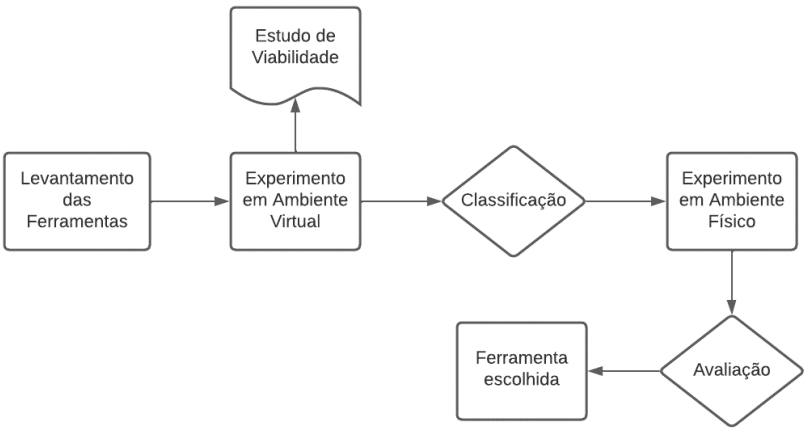
Por fim, além dos critérios anteriores, a aplicação das ferramentas nos laboratórios de informática da UFES Campus Alegre é o ponto fundamental em termos de qualidade da entrega deste trabalho.

3. METODOLOGIA

A metodologia adotada neste estudo envolveu uma série de etapas para avaliar e selecionar a melhor ferramenta de gerenciamento de configuração de redes para os Laboratórios de Informática da UFES - Campus Alegre. Inicialmente, foi realizado um levantamento das ferramentas disponíveis no mercado. A próxima etapa consistiu na realização de experimentos computacionais. As ferramentas selecionadas foram instaladas em uma máquina virtual, onde puderam ser avaliadas de acordo com os critérios estabelecidos. Durante esses experimentos, foram coletados dados e impressões sobre cada ferramenta, registrando-se informações relevantes sobre o processo de instalação e configuração, bem como a facilidade de uso e recursos oferecidos.

Com base nos resultados dos experimentos, as duas ferramentas com melhor desempenho foram selecionadas para a próxima fase. Essas ferramentas foram instaladas e avaliadas em um ambiente físico e controlado. Na avaliação prática pode-se verificar o desempenho das ferramentas em condições reais de execução, considerando a instalação na rede física e as necessidades específicas dos laboratórios. Foram analisados os dados coletados, as impressões obtidas e as necessidades específicas dos laboratórios. Com base nessas informações, obteve-se uma análise da ferramenta que melhor atendeu às demandas de gerenciamento de configuração de redes dos Laboratórios de Informática da UFES - Campus Alegre. Na Figura 03, são apresentadas as etapas do projeto, ilustrando o fluxo de execução da metodologia.

Figura 03: Etapas do Projeto



Fonte: Autor

No primeiro experimento, as ferramentas (ZABBIX, CACTI, PRTG e SOLARWINDS) foram avaliadas de acordo com as métricas descritas na sessão 2.4.2. Cada métrica possui seu método de avaliação específico. O grau de dificuldade da instalação foi avaliado em uma escala de 1 a 5, sendo 1 indicando uma instalação fácil e 5 indicando uma instalação difícil. O tempo total de instalação foi medido em minutos.

Para a descoberta automática de dispositivos, foi verificado se cada ferramenta possui esse recurso. A configuração foi avaliada considerando a facilidade e flexibilidade oferecida por cada ferramenta. O grau de dificuldade na configuração também recebeu a pontuação em uma escala de 1 a 5.

A interface gráfica foi avaliada com base na usabilidade e clareza, considerando o quão fácil é navegar e entender as informações apresentadas. Essa avaliação foi realizada em uma escala de 1 a 5, sendo 1 o nível mais baixo e 5 o mais alto, refletindo o grau de facilidade de uso e compreensão. O nível de acesso à informação também foi avaliado em uma escala de 1 a 5, analisando como as informações foram apresentadas e se eram intuitivas para o usuário.

Essas avaliações foram realizadas na primeira etapa do experimento, permitindo comparar e analisar as métricas de cada ferramenta e obter informações para a seleção da ferramenta mais adequada para os laboratórios de informática da UFES. Na tabela a seguir podemos visualizar o método de avaliação de cada métrica.

Tabela 1 - Método de avaliação

Métricas	**Método de avaliação**
Implementação	
Grau de Dificuldade da Instalação	Pontuação de 1 a 5, sendo 1 fácil e 5 difícil
Tempo (minutos)	Medir o tempo total de instalação em minutos
Configuração	
Descoberta Automática	Verificar se a ferramenta possui recurso de descoberta automática
Configuração	Avaliar a facilidade e flexibilidade na configuração

Grau de Dificuldade	Pontuação de 1 a 5, sendo 1 fácil e 5 difícil
Funcionamento	
Interface Gráfica	Avaliar a usabilidade e clareza da interface
Nível de Acesso à Informação	Verificar como as informações são apresentadas e se são intuitivas
Impressões	Análise geral

Fonte: Autor

Nesta etapa do experimento, cada ferramenta foi instalada em uma máquina virtual sem configurações prévias. Em seguida, uma pequena rede virtual foi configurada nesse ambiente para simular uma rede física. Assim foi possível observar o processo de instalação e configuração de cada ferramenta.

Os campos "Grau de Dificuldade da Instalação" e "Tempo (minutos)" foram preenchidos com informações sobre a dificuldade percebida durante a instalação de cada ferramenta e o tempo total necessário para concluir a instalação.

A presença ou ausência de descoberta automática de dispositivos foi registrada na coluna "Descoberta Automática". Em seguida, foi observado a facilidade e flexibilidade da configuração de cada ferramenta e registrado o grau de dificuldade percebido.

Por fim, na coluna "Impressões", registrou-se as impressões gerais sobre cada ferramenta, incluindo observações sobre o processo de instalação e configuração, facilidade de uso, recursos oferecidos e qualquer outra informação relevante.

A Tabela 2 será preenchida com os dados coletados e as impressões obtidas durante o experimento, de forma a permitir uma análise qualitativa das ferramentas para a seleção da mais adequada para os laboratórios de informática da UFES.

Tabela 2 - Comparação

Ferramenta	ZABBIX	CACTI	PRTG	SOLARWINDS
Grau de Dificuldade da Instalação	-	-	-	-
Tempo (minutos)	-	-	-	-
Descoberta Automática	-	-	-	-
Configuração	-	-	-	-
Grau de Dificuldade	-	-	-	-
Interface Gráfica	-	-	-	-
Nível de Acesso à Informação	-	-	-	-
Impressões	-	-	-	-

Fonte: Autor

Com base nos resultados dos primeiros experimentos computacionais e levando em consideração os critérios estabelecidos, foram selecionadas as duas ferramentas com melhor desempenho. Essas ferramentas foram avaliadas em um ambiente físico e controlado dentro do Laboratório de Desenvolvimento de *Software* 2. Essa etapa permitiu medir o desempenho das ferramentas em situações reais, levando em consideração a instalação na rede física e as condições de trabalho dos componentes e sistemas em operação.

A avaliação em ambiente físico propiciou uma oportunidade de verificar se as ferramentas selecionadas atendem às expectativas e se seriam capazes de lidar com os desafios e demandas reais dos Laboratórios de Informática da UFES - Campus Alegre. Sendo possível avaliar não apenas a funcionalidade das ferramentas, mas também sua adaptabilidade, estabilidade e capacidade de integração com o ambiente existente.

4. RESULTADOS E DISCUSSÃO

Nesta seção, são apresentados os resultados obtidos através dos testes realizados tanto em ambiente virtual quanto em ambiente físico. E são descritas as configurações específicas utilizadas, bem como todos os procedimentos adotados e comportamentos observados durante a experimentação.

4.1. TESTE VIRTUAL

A primeira etapa deste estudo envolveu a condução de experimentos em um ambiente virtual, conforme descrito na metodologia. Esta seção detalha o processo, as configurações adotadas, os procedimentos executados durante os testes e os resultados observados.

4.2. TESTE VIRTUAL: ZABBIX

A primeira ferramenta de gestão de configuração de redes avaliada foi o *Zabbix*. O *software* está disponível para *download* no *site* oficial, onde o usuário pode selecionar a configuração de máquina apropriada para hospedar o servidor da ferramenta.

Nesta avaliação, optou-se pela versão 6.4 do *Zabbix*, projetada especificamente para o *Ubuntu* 22.04, com suporte ao banco de dados *MySQL* e à interface *web* utilizando o servidor *Apache*, conforme ilustrado na Figura 04. Vale destacar que o *Zabbix* requer que as estações de gerenciamento sejam baseadas em sistemas operacionais *Linux*, o que pode representar uma limitação para alguns ambientes corporativos.

Figura 04: Configuração de download *Zabbix*

Fonte: Autor

A seguir, apresenta-se um exemplo *de script* com os comandos que foram executados no terminal para instalar e configurar o Zabbix:

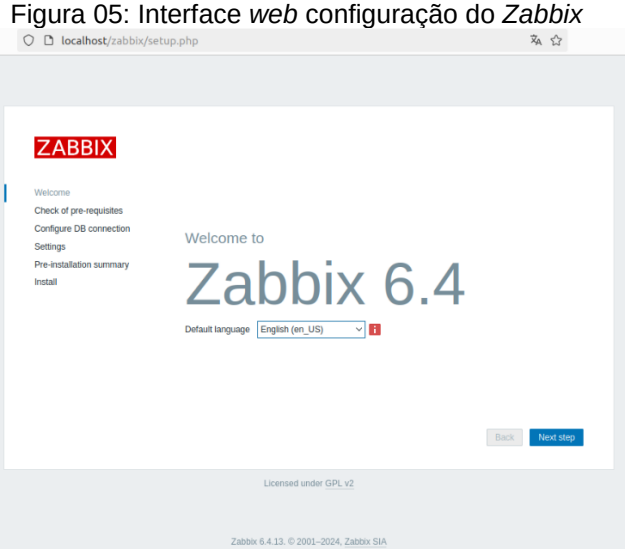
```
1    /* Instalando o repositório Zabbix */
2    wget      https://repo.zabbix.com/zabbix/6.4/ubuntu/pool/main/z/zabbix-
     release/zabbix-release_6.4-1+ubuntu22.04_all.deb
3    dpkg -i zabbix-release_6.4-1+ubuntu22.04_all.deb

4    /* Atualizando os pacotes do sistema */
5    apt update

6    /* Instalando o servidor Zabbix, frontend e agente */
7    apt install zabbix-server-mysql zabbix-frontend-php zabbix-apache-conf
     zabbix-sql-scripts zabbix-agent

8    /* Criar banco de dados inicial */
9    mysql -uroot -p
10   adm01
11   mysql> create database zabbix character set utf8mb4 collate utf8mb4_bin;
12   mysql> create user zabbix@localhost identified by 'senhaforte123';
13   mysql> grant all privileges on zabbix.* to zabbix@localhost;
14   mysql> set global log_bin_trust_function_creators = 1;
15   mysql> quit;

16   /* Importação do esquema inicial e os dados */
17   zcat /usr/share/doc/zabbix-server-mysql*/create.sql.gz | mysql -uzabbix
     -p Zabbix

18   /* Configurando o banco de dados para o servidor Zabbix */
19   /* Editar arquivo /etc/zabbix/zabbix_server.conf */

20   sudo nano /etc/zabbix/zabbix_server.conf
21   DBName=zabbix
22   DBUser=zabbix
23   DBPassword=senhaforte123

24   /* Iniciando o servidor Zabbix e os processos do agente */
25   systemctl restart zabbix-server zabbix-agent apache2
26   systemctl enable zabbix-server zabbix-agent apache2

27   /* A partir de agora podemos abrir a página Web do Zabbix */
28   http://localhost/zabbix
```

Os comandos acima configuram o ambiente necessário para a operação do *Zabbix*, incluindo a criação de um banco de dados *MySQL*, essencial para o armazenamento dos dados coletados pela ferramenta.

A interface do sistema foi acessada com sucesso após a conclusão do processo de instalação, como demonstrado na Figura 05. O procedimento de instalação, embora tecnicamente direto, apresentou desafios adicionais devido à falta de familiaridade com o sistema operacional *Linux*. Comandos como a instalação de pacotes, edição de arquivos de configuração e gerenciamento de permissões exigiram tempo e

pesquisa adicional, aumentando significativamente o tempo total de instalação, que foi de aproximadamente 3 horas e 30 minutos.

Figura 05: Interface *web* configuração do *Zabbix*



Fonte: Autor

Como usuário mais familiarizado com o sistema operacional *Windows* e com experiência limitada com o *Linux* acrescentou uma camada extra de dificuldade à instalação do *Zabbix*. Encontrar e executar comandos no terminal, como instalar pacotes, editar arquivos de configuração e gerenciar permissões, foi uma tarefa que exigiu maior tempo e pesquisa externa na *internet*. Lidar com a configuração do *MySQL* e questões relacionadas às políticas de senha e permissões representaram desafios adicionais, especialmente ao encontrar erros como "*Table 'role' already exists*". No entanto, foi possível concluir com êxito a instalação do *Zabbix*. Devido à inexperiência do autor com o *Linux*, o processo de instalação levou aproximadamente 3 horas e 30 minutos.

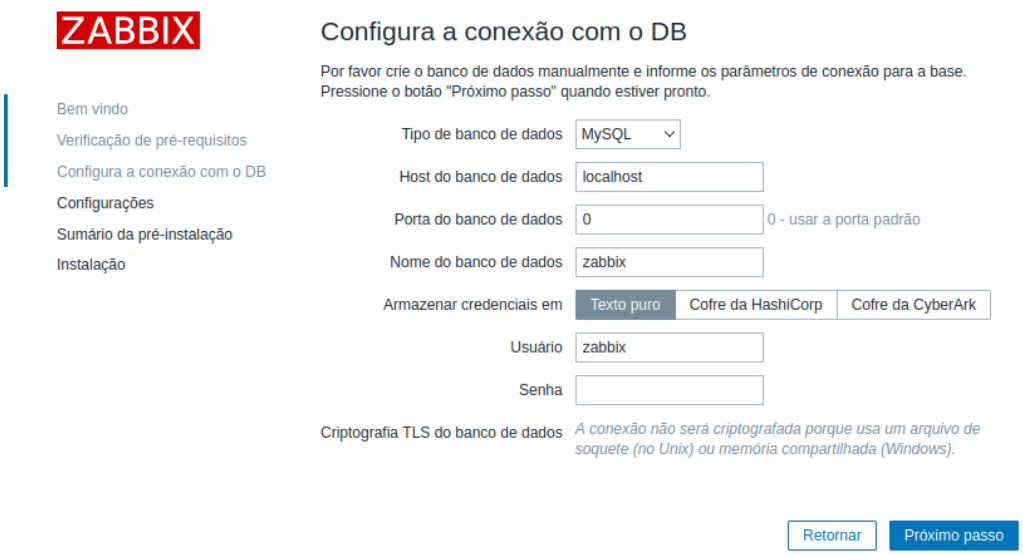
Na página que encontramos como fazer a instalação do *Zabbix*, temos acesso fácil a documentação de todo o sistema, para este trabalho foi utilizado a versão traduzida para o Português fornecida pelo *Google Tradutor*. Assim iniciamos a configuração da interface *web* do *Zabbix*. Essa interface foi acessada pelo navegador de *internet* em *localhost/zabbix*, como mostrado na Figura 04. No primeiro passo foi feita a verificação dos pré-requisitos do sistema e componentes para o funcionamento da ferramenta, como podemos observar na Figura 06 a seguir.

Figura 06: Interface inicial do *Zabbix*

Fonte: Autor

O próximo passo foi configurar a conexão com o banco de dados configurado no momento da instalação. Então selecionamos o tipo de banco de dados como *MySQL*, identificamos o *host* como *local host*, deixamos como padrão a porta do banco de dados, inserimos o nome que demos ao banco de dados além do usuário e senha, essa configuração pode ser visualizada na Figura 07 a seguir.

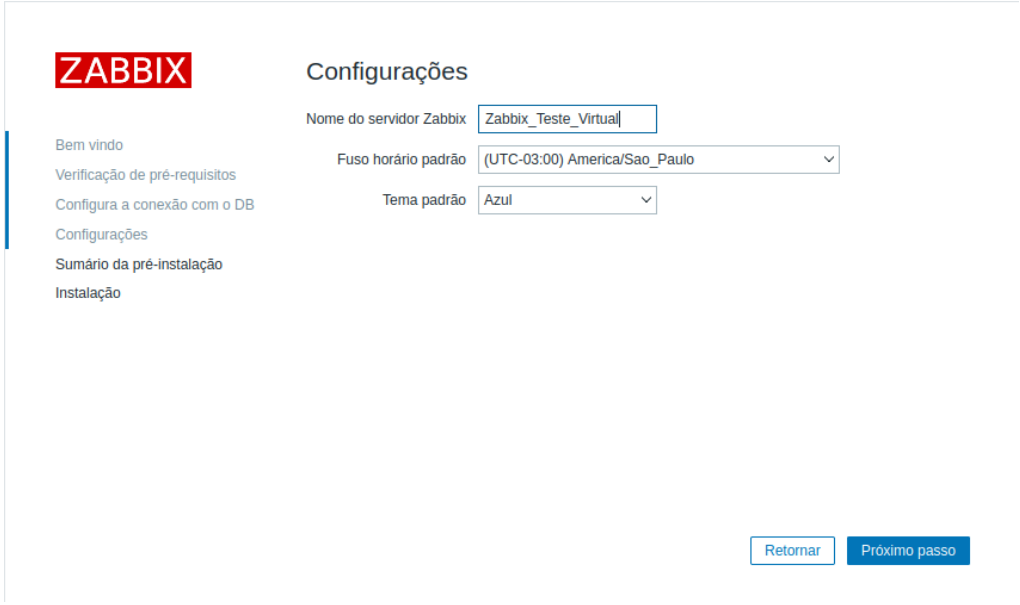
Figura 07: Configuração com o Banco de Dados



Fonte: Autor

Após configurar a conexão com o banco de dados, foi necessário nomear o servidor *Zabbix* e ajustar o fuso horário, como ilustrado na Figura 08. Este é o passo final na configuração inicial da interface web.

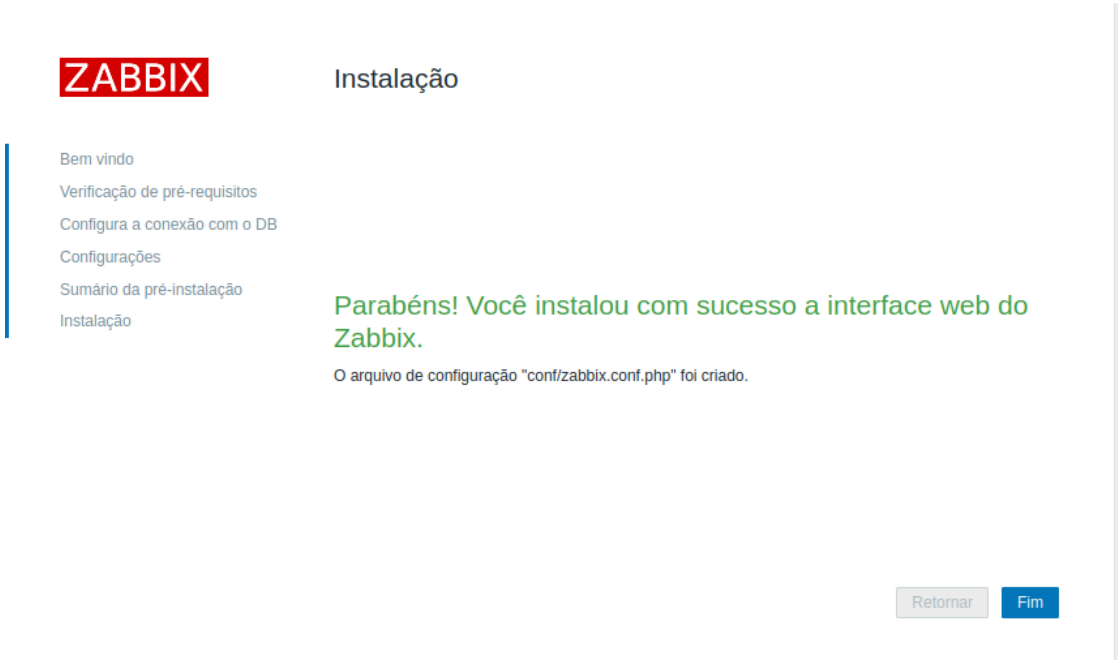
Figura 08: Configurações finais



Fonte: Autor

Concluídos todos os passos, a instalação da interface *web* do *Zabbix* foi finalizada com sucesso, como ilustrado nas Figuras 09.

Figura 09: Instalação concluída



Fonte: Autor

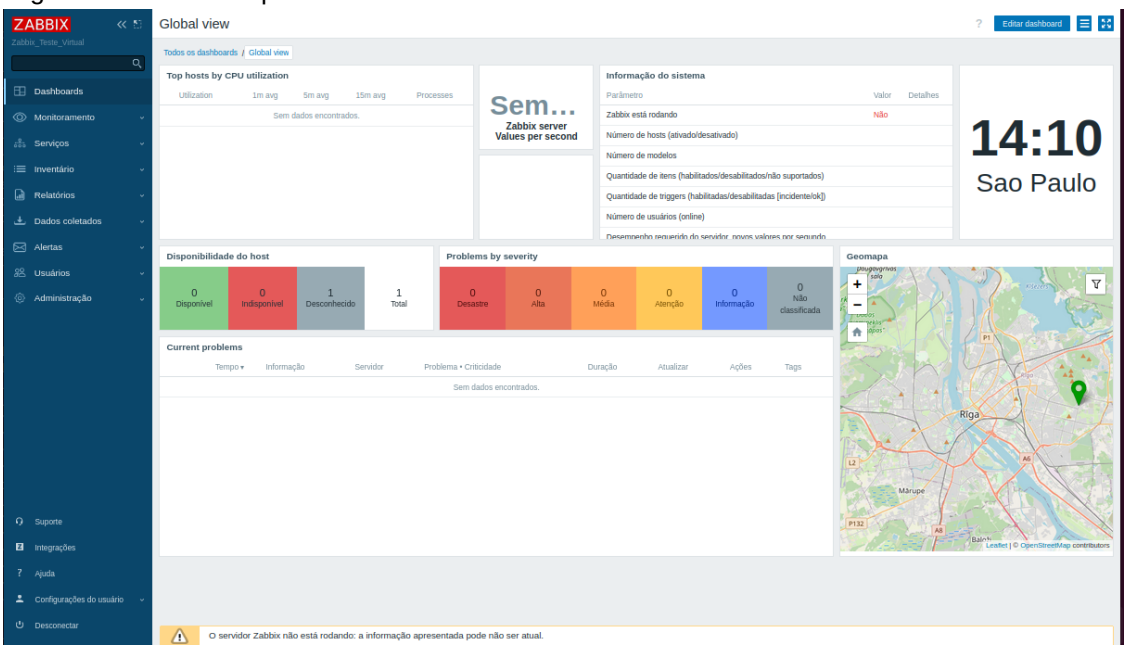
O primeiro login no *Zabbix* foi realizado utilizando as credenciais de administrador padrão, com o nome de usuário "Admin" e senha "zabbix", como ilustrado na Figura 10.

Figura 10: Tela de Login

Fonte: Autor

Após o *login*, o *dashboard* inicial foi exibido, mostrando diversos indicadores, porém sem configuração inicial, como visto na Figura 11. Este *dashboard* serve como ponto de partida para a personalização e monitoramento dos componentes da rede.

Figura 11: Tela Principal

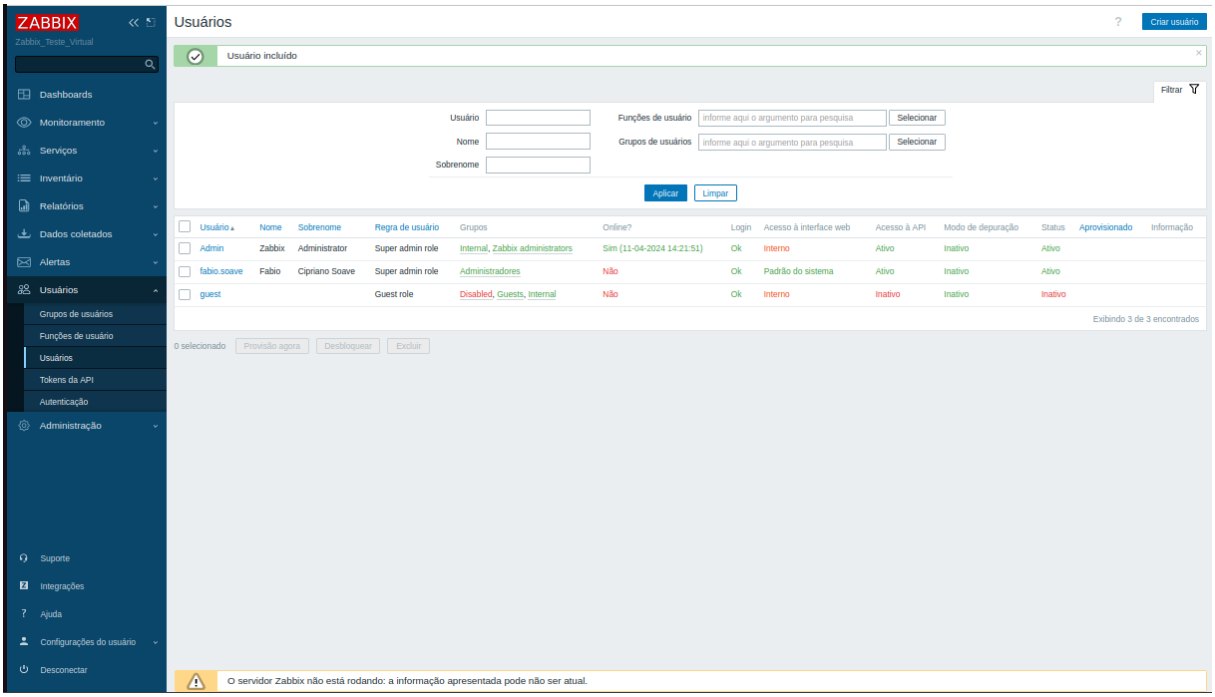


Fonte: Autor

O próximo passo foi a exploração do menu Usuários, onde o *Zabbix* permite a criação de grupos de usuários, grupos de permissões, e a configuração personalizada de cada

permissão. A ferramenta também permite ativar ou inativar usuários. Na Figura 12, podemos observar os usuários criados, incluindo o usuário Admin padrão, um Convidado (*guest*), e um novo usuário com privilégios de Super Administrador.

Figura 12: Lista de usuários no *Zabbix*



Fonte: Autor

Com a exploração do sistema, iniciou-se o processo de descoberta dos *hosts*, que são os equipamentos, serviços e passivos da rede a serem monitorados. A instalação do Agente do *Zabbix* nos servidores *Linux Ubuntu*, hospedados na máquina virtual, foi realizada com os seguintes comandos:

```
sudo apt update
sudo apt install zabbix-agent
sudo nano /etc/zabbix/zabbix_agentd.conf
Server=192.168.36.64
ServerActive=192.168.36.64
Hostname=ServerUbuntu1
sudo systemctl restart zabbix-agent
sudo systemctl status zabbix-agent
```

A Figura 13 mostra a edição do arquivo *zabbix_agentd.conf* com os parâmetros do servidor, passo essencial para garantir a comunicação adequada entre o agente e o servidor.

Figura 13: Configuração arquivo *zabbix_agentd.conf*

```
ServerUbuntu2 [Executando] - Oracle VM VirtualBox
Arquivo  Máquina  Visualizar  Entrada  Dispositivos  Ajuda
  GNU nano 6.2                    /etc/zabbix/zabbix_agentd.conf *
#       Internal alias for AllowKey/DenyKey parameters depending on value:
#       0 - DenyKey=system.run[*]
#       1 - AllowKey=system.run[*]
#
# Mandatory: no

### Option: LogRemoteCommands
#       Enable logging of executed shell commands as warnings.
#       0 - disabled
#       1 - enabled
#
# Mandatory: no
# Default:
# LogRemoteCommands=0

##### Passive checks related

### Option: Server
#       List of comma delimited IP addresses, optionally in CIDR notation, or DNS names of Zabbix s>
#       Incoming connections will be accepted only from the hosts listed here.
#       If IPv6 support is enabled then '127.0.0.1', '::127.0.0.1', '::ffff:127.0.0.1' are treated >
#       and '::/0' will allow any IPv4 or IPv6 address.
#       '0.0.0.0/0' can be used to allow any IPv4 address.
#       Example: Server=127.0.0.1,192.168.1.0/24,::1,2001:db8::/32,zabbix.example.com
#
# Mandatory: yes, if StartAgents is not explicitly set to 0
# Default:
# Server=

Server=192.168.36.64

### Option: ListenPort
#       Agent will listen on this port for connections from the server.
File to insert [from ./]:
^G Help          M-F New Buffer      ^X Execute Command
^C Cancel        M-N No Conversion   ^T Browse
Right Control
Right Control
```

Fonte: Autor

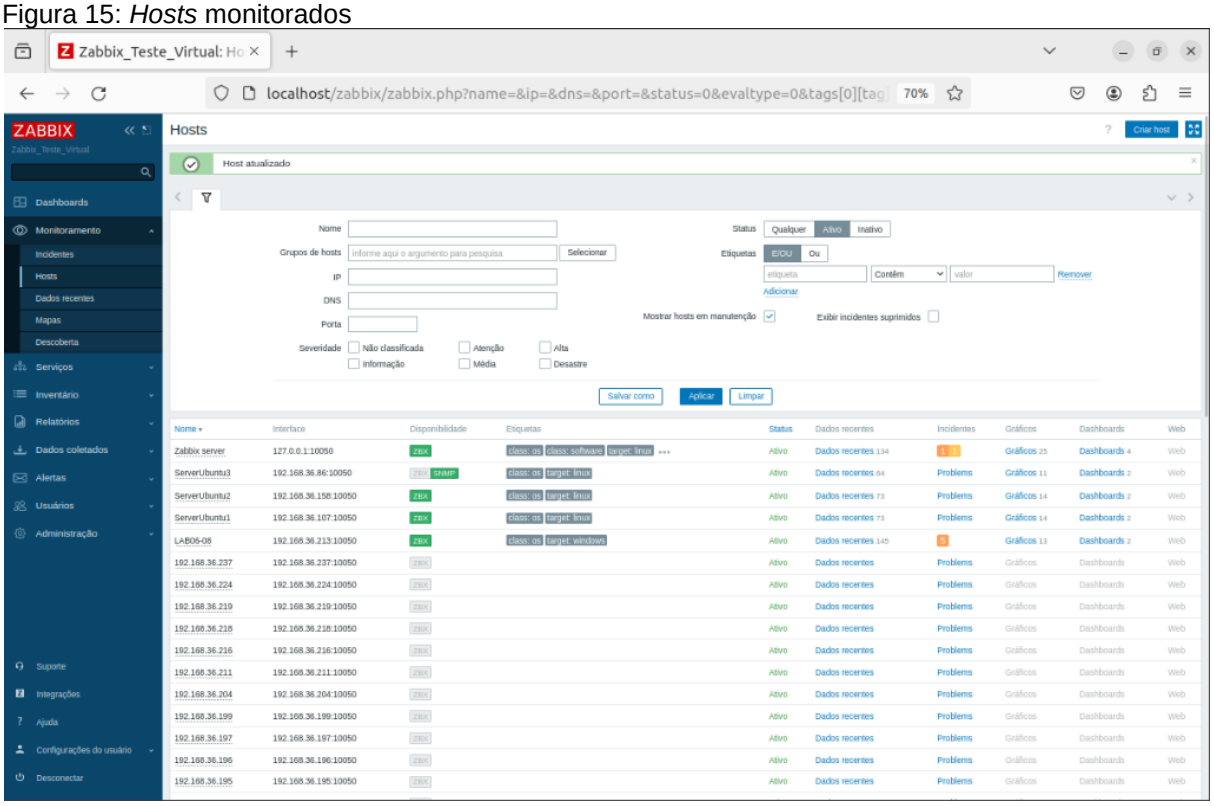
Após a instalação e configuração do agente *Zabbix*, como ilustrado na Figura 14, o agente foi ativado corretamente.

Figura 14: Agente *Zabbix* ativo

```
ServerUbuntu2 [Executando] - Oracle VM VirtualBox
Arquivo  Máquina  Visualizar  Entrada  Dispositivos  Ajuda
adm01@linuxserver01:~$ sudo systemctl restart zabbix-agent
adm01@linuxserver01:~$ sudo systemctl enable zabbix-agent
Synchronizing state of zabbix-agent.service with SysV service script with /lib/systemd/systemd-sysv-
install.
Executing: /lib/systemd/systemd-sysv-install enable zabbix-agent
adm01@linuxserver01:~$ sudo systemctl status zabbix-agent
● zabbix-agent.service - Zabbix Agent
     Loaded: loaded (/lib/systemd/system/zabbix-agent.service; enabled; vendor preset: enabled)
     Active: active (running) since Thu 2024-04-18 20:07:49 UTC; 36s ago
   Main PID: 1259 (zabbix_agentd)
      Tasks: 6 (limit: 2221)
     Memory: 5.9M
        CPU: 42ms
     CGroup: /system.slice/zabbix-agent.service
             ├─1259 /usr/sbin/zabbix_agentd -c /etc/zabbix/zabbix_agentd.conf
             ├─1260 "/usr/sbin/zabbix_agentd: collector [idle 1 sec]" "" "" "" "" "" "" "" "" "" "" "" ""
             ├─1261 "/usr/sbin/zabbix_agentd: listener #1 [waiting for connection]"
             ├─1262 "/usr/sbin/zabbix_agentd: listener #2 [waiting for connection]"
             ├─1263 "/usr/sbin/zabbix_agentd: listener #3 [waiting for connection]"
             └─1264 "/usr/sbin/zabbix_agentd: active checks #1 [idle 1 sec]" "" "" "" "" "" "" "" "" "" "" "" "
```

configurando-se uma regra de descoberta baseada em um intervalo de *IPs* disponíveis na rede. Em poucos minutos, o *Zabbix* identificou vários dispositivos além dos previamente cadastrados, como ilustrado na Figura 15.

Figura 15: *Hosts* monitorados

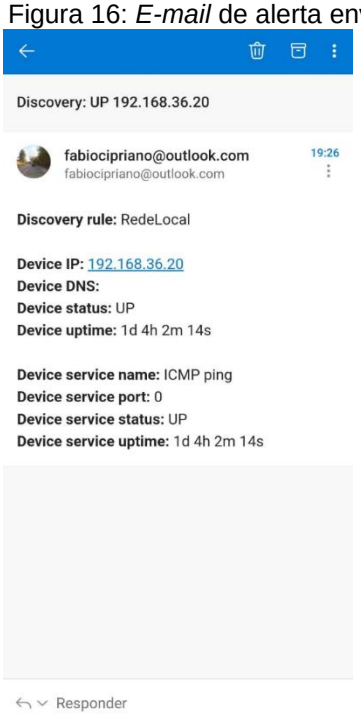


Fonte: Autor

A Figura 15 mostra que alguns *hosts* estão ativos (com a Disponibilidade *ZBX* em verde), enquanto outros ainda não estão completamente configurados, indicando a necessidade de instalação do Agente *Zabbix*. O *Zabbix* também oferece procedimentos automáticos pré-configurados para detectar e relatar problemas em *hosts*, demonstrando uma funcionalidade robusta.

O *Zabbix* permite a criação de Grupos de *Hosts*, possibilitando a organização dos *hosts* monitorados de acordo com critérios específicos, como laboratórios de computadores ou grupos de serviços e equipamentos. No menu Alertas, é possível configurar alertas específicos para qualquer atividade no *Zabbix*. Como teste, foi configurado um alerta para notificar via e-mail quando um novo *host* fosse identificado pelo *IP*, além de adicionar automaticamente esse *host* ao painel de monitoramento. A Figura 16 mostra um exemplo de *e-mail* de alerta enviado, destacando a alta personalização dos parâmetros.

Figura 16: *E-mail* de alerta enviado



Fonte: Autor

A avaliação do *Zabbix* demonstrou ser uma ferramenta robusta e altamente configurável para a gestão e monitoramento de redes, com um leque extenso de funcionalidades voltadas para o gerenciamento detalhado de *hosts* e serviços. Apesar de apresentar uma curva de aprendizado acentuada, especialmente para usuários menos familiarizados com o sistema operacional *Linux*, a instalação e configuração do *Zabbix* revelaram-se eficazes, permitindo a detecção automática de dispositivos na rede e a configuração personalizada de alertas e permissões. A experiência destaca a importância de conhecimento técnico prévio para maximizar o uso do *Zabbix*, mas também reforça seu potencial como uma solução abrangente para ambientes complexos.

4.2.1. PROCEDIMENTOS EXECUTADOS: ZABBIX

Durante a configuração e utilização do *Zabbix* no ambiente de teste virtual, uma série de procedimentos foram realizados para avaliar sua eficácia no gerenciamento de configuração, *backup* e inventário. Inicialmente, foi realizada a instalação do *Zabbix Server* em uma máquina virtual utilizando o sistema operacional *Linux* (*Ubuntu* 20.04). A instalação incluiu a configuração de um servidor *web Apache*, um banco de dados *MySQL* e o *PHP*, componentes essenciais para o funcionamento do *Zabbix*. Após a

instalação, o servidor *Zabbix* foi iniciado e acessado via interface *web* para concluir as configurações iniciais.

Um banco de dados *MySQL* dedicado foi configurado para armazenar todos os dados monitorados e gerenciados pelo *Zabbix*, com *backups* automáticos programados para garantir a integridade e recuperação dos dados em caso de falhas. Em seguida, foram instalados e configurados agentes *Zabbix* em máquinas virtuais adicionais, responsáveis por coletar dados de desempenho e *status* dos dispositivos na rede. Esses agentes foram configurados para enviar informações regularmente ao servidor *Zabbix*, permitindo um monitoramento contínuo e centralizado.

Cada dispositivo foi configurado com parâmetros específicos de monitoramento, como uso de *CPU*, memória, espaço em disco e disponibilidade de rede. Para facilitar a configuração de novos dispositivos e padronizar as métricas coletadas, foram utilizados *templates* de monitoramento.

A funcionalidade de inventário automático foi habilitada, permitindo que o *Zabbix* coletasse e organizasse informações detalhadas sobre o *hardware* e *software* dos dispositivos monitorados. Relatórios periódicos de inventário foram gerados, contendo detalhes como versões de *software*, configurações de *hardware* e alterações realizadas. Além disso, regras de automação foram configuradas para realizar *backups* automáticos das configurações de dispositivos críticos, e alertas foram criados para notificar os administradores de rede sobre falhas, desempenho inadequado ou alterações não autorizadas nas configurações dos dispositivos monitorados.

Os procedimentos de *backup* incluíram a programação de *backups* regulares do banco de dados do *Zabbix* e das configurações do sistema, com testes de recuperação realizados para garantir a eficácia da restauração de dados em caso de necessidade. Relatórios detalhados foram gerados utilizando as funções de relatório do *Zabbix*, abordando aspectos como desempenho, histórico de eventos e inventário de *hardware* e *software*. Esses relatórios foram analisados para avaliar a clareza e utilidade das informações para o gerenciamento das redes nos laboratórios.

Finalmente, o *Zabbix* foi configurado para rastrear e auditar todas as alterações de configuração realizadas nos dispositivos monitorados, com *logs* detalhados sendo

revisados para garantir que todas as mudanças fossem registradas e documentadas adequadamente. Esses procedimentos permitiram uma avaliação abrangente do *Zabbix* no contexto do gerenciamento de configuração, *backup*, inventário e monitoramento em um ambiente de laboratório simulado.

4.2.2. COMPORTAMENTOS OBSERVADOS: ZABBIX

Os resultados observados durante a implementação do *Zabbix* no ambiente de testes virtuais destacam tanto os pontos fortes quanto os desafios encontrados ao utilizar essa ferramenta para o gerenciamento de configuração, *backup* e inventário.

Em termos de instalação, o *Zabbix* apresentou um grau de dificuldade relativamente elevado, classificado como 4 em uma escala de 1 a 5, onde 5 representa o máximo de dificuldade. Isso se deve, em grande parte, à complexidade envolvida na configuração inicial do servidor *Zabbix*, que requer o domínio de comandos no sistema operacional *Linux*, bem como a configuração manual de componentes como o servidor *Apache*, o banco de dados *MySQL* e o *PHP*. O processo de instalação demandou aproximadamente 240 minutos, o que inclui tanto a instalação dos pacotes necessários quanto a configuração inicial do sistema.

Um ponto positivo observado foi a funcionalidade de descoberta automática, que, apesar de requerer a configuração manual de regras específicas, funcionou de maneira eficaz após a sua implementação. Isso permitiu que o *Zabbix* identificasse e começasse a monitorar automaticamente dispositivos conectados à rede, um recurso fundamental para o gerenciamento eficiente de grandes infraestruturas.

A configuração geral do *Zabbix*, incluindo a adição de dispositivos e a aplicação de *templates* de monitoramento, foi realizada com sucesso, seguindo a documentação fornecida. Embora a curva de aprendizado possa ser íngreme para usuários sem experiência prévia com *Linux* ou sistemas de monitoramento complexos, a documentação oficial fornecida pelo *Zabbix* mostrou-se adequada para guiar o processo de configuração.

O grau de dificuldade para a configuração foi avaliado como 3 em uma escala de 1 a 5, o que reflete um nível de complexidade moderado. No entanto, a interface gráfica

do *Zabbix* se destacou pela sua usabilidade e facilidade de compreensão. A interface gráfica do Zabbix foi facilmente compreendida, facilitando a navegação e o acesso às informações essenciais. Essa usabilidade intuitiva é um ponto crucial para administradores de rede, que precisam monitorar e gerenciar múltiplos dispositivos de maneira eficiente.

O nível de acesso à informação também foi classificado como extremamente fácil, com o *Zabbix* proporcionando uma apresentação clara e acessível dos dados monitorados. A interface permite que os administradores acessem rapidamente informações detalhadas sobre o *status* e o desempenho dos dispositivos, bem como dados de inventário e *logs* de eventos.

As impressões gerais sobre o *Zabbix* foram positivas, apesar dos desafios iniciais de instalação e configuração. Para usuários que não estão acostumados com o uso do *Linux*, o processo pode parecer um pouco complexo, mas seguindo o manual e a documentação oficial, a instalação pode ser realizada sem grandes problemas. A instalação do agente *Zabbix* foi rápida, permitindo que o sistema começasse a monitorar os hosts em poucos minutos. A interface intuitiva facilita a familiarização com o sistema e a configuração do servidor, tornando o *Zabbix* uma ferramenta acessível para o gerenciamento de redes nos Laboratórios de Informática da UFES.

Esses resultados demonstram que, apesar de alguns desafios iniciais, o *Zabbix* oferece uma solução robusta e eficaz para o gerenciamento de configuração, inventário e monitoramento em ambientes complexos, com um equilíbrio adequado entre funcionalidades avançadas e facilidade de uso.

4.3. TESTE VIRTUAL: CACTI

O *Cacti* é uma ferramenta de código aberto amplamente utilizada para monitoramento de redes, que se destaca por suas capacidades de coleta e visualização de dados em gráficos. Este teste foi conduzido para avaliar as funcionalidades do *Cacti*, bem como sua adequação para a gestão de configuração de redes. A instalação e configuração do *Cacti* foram realizadas em um ambiente *Linux*, utilizando-se o *Ubuntu* 22.04 como sistema operacional, seguindo as instruções fornecidas na documentação oficial.

A primeira etapa do processo de instalação envolveu a atualização dos pacotes do sistema e a instalação das dependências necessárias para o funcionamento do *Cacti*. Os seguintes comandos foram executados no terminal para realizar essas tarefas:

```
1    sudo apt update
2    sudo apt upgrade -y
3    sudo apt install apache2 mariadb-server php php-mysql libapache2-mod-php php
```

Com as dependências instaladas, o próximo passo foi configurar o banco de dados *MySQL* (*MariaDB*). O banco de dados é essencial para armazenar as informações de monitoramento coletadas pelo *Cacti*. A configuração foi realizada com os seguintes comandos:

```
1    sudo mysql -u root -p
2    CREATE DATABASE cacti;
3    CREATE USER 'cactiuser'@'localhost' IDENTIFIED BY 'adm01';
4    GRANT ALL PRIVILEGES ON cacti.* TO 'cactiuser'@'localhost';
5    FLUSH PRIVILEGES;
6    EXIT;
```

Após configurar o banco de dados, foi necessário importar o esquema inicial para o banco de dados do *Cacti*:

```
1    sudo mysql -u cactiuser -p cacti < /usr/share/doc/cacti/cacti.sql
```

Com o banco de dados configurado, o próximo passo foi configurar o *Cacti* para que ele pudesse se comunicar com o banco de dados e começar a coletar dados. O arquivo de configuração foi editado para definir as credenciais do banco de dados:

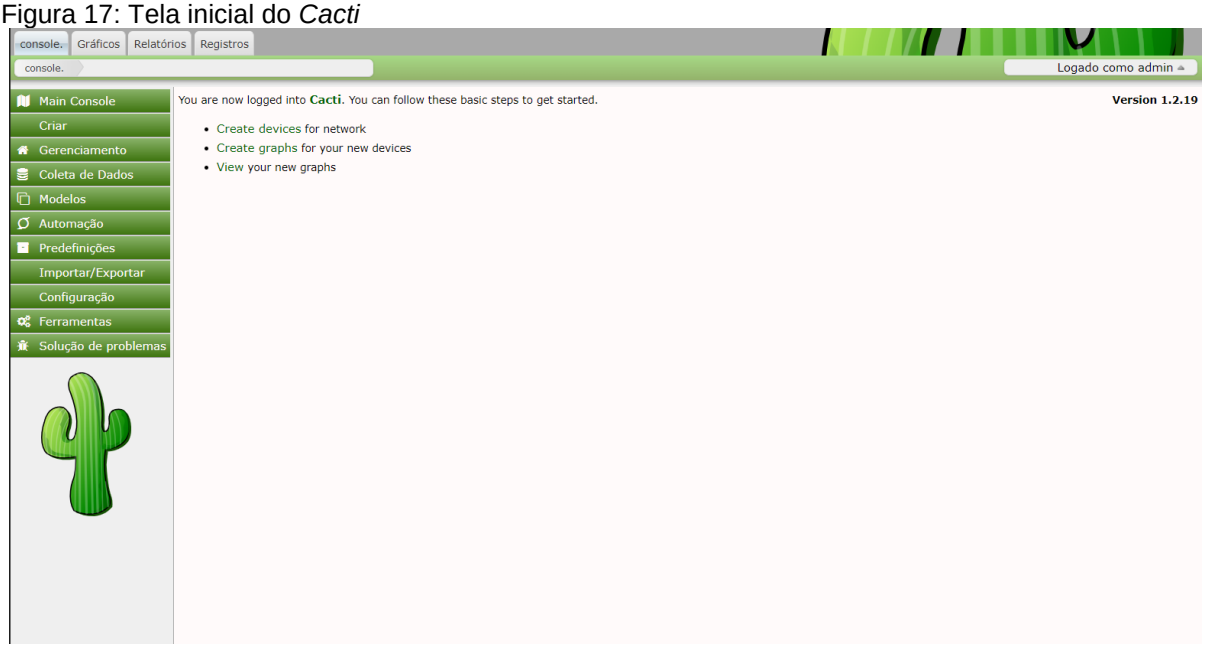
```
1    sudo nano /etc/cacti/debian.php
2    # Adicionar as linhas para configurar o banco de dados
3    $database_type = "mysql";
4    $database_default = "cacti";
5    $database_hostname = "localhost";
6    $database_username = "cactiuser";
7    $database_password = "adm01";
8    $database_port = "3306";
```

Depois de configurar o arquivo de banco de dados, o *Apache* foi reiniciado para aplicar as mudanças:

```
1    sudo systemctl restart apache2
```

Finalmente, o acesso à interface *web* do *Cacti* foi configurado. A interface *web* é crucial para gerenciar e visualizar os dados coletados. Para acessar a interface, basta abrir um navegador e acessar o endereço http://localhost/cacti. Na primeira execução, o assistente de instalação do *Cacti* guiou o processo de configuração inicial, como a verificação de pré-requisitos do sistema, configuração do administrador e importação de templates padrão. A Figura 17 abaixo mostra a tela inicial do *Cacti* após concluída toda a instalação.

Figura 17: Tela inicial do *Cacti*



Fonte: Autor

A configuração do *Cacti* revelou-se muito desafiadora, demandando um esforço significativo para ser concluída com sucesso. O processo envolveu diversas etapas complexas que exigiram a consulta a vários tutoriais e fóruns *online*, dado que a documentação oficial nem sempre fornecia informações suficientemente claras ou detalhadas para resolver todos os problemas encontrados. Essa dificuldade evidenciou a necessidade de uma curva de aprendizado acentuada para uso total da ferramenta.

4.3.1. PROCEDIMENTOS EXECUTADOS: CACTI

Durante a análise do *Cacti*, foram exploradas diversas funcionalidades cruciais para a gestão e monitoramento de redes de computadores. Inicialmente, a configuração de usuários foi investigada, onde foi possível estabelecer diferentes níveis de permissão, permitindo a delegação de tarefas de monitoramento e administração de forma segura e controlada. Este recurso, mostrou-se robusto, garantindo que cada usuário tenha acesso apenas às áreas necessárias para suas funções.

O gerenciamento de dispositivos foi testado através da funcionalidade de *Device Management*, onde o *Cacti* possibilitou a adição e configuração detalhada de dispositivos de rede. Durante o processo, utilizou-se a ferramenta de descoberta de dispositivos (*Device Discovery*), que permitiu a identificação automática de dispositivos na rede, simplificando a inclusão de novos elementos para monitoramento.

A criação e personalização de gráficos foi um dos pontos fortes observados no Cacti. A plataforma oferece uma ampla gama de opções para a geração de gráficos detalhados, permitindo a visualização em tempo real do desempenho dos dispositivos monitorados. Essa capacidade de personalização é essencial para uma análise detalhada, sendo possível ajustar os gráficos para atender às necessidades específicas de monitoramento.

Em relação à gestão de configuração, foi avaliado se o *Cacti* oferece recursos nativos para este fim. Contudo, constatou-se que o *Cacti* não possui uma funcionalidade direta para a gestão de configuração, o que limita sua aplicabilidade em cenários onde essa capacidade é crucial. Para contornar essa limitação, seria necessário integrar o *Cacti* com outras ferramentas especializadas nesse tipo de gestão.

Além disso, foi explorada a funcionalidade de *backup*, essencial para garantir a segurança dos dados monitorados. No entanto, foi identificado que o *Cacti* não dispõe de uma solução integrada para *backup*, exigindo a configuração manual ou a utilização de *scripts* e ferramentas externas para essa finalidade.

Por fim, o estudo das funcionalidades do *Cacti* evidenciou suas capacidades e limitações. Enquanto a ferramenta se destaca em monitoramento e visualização de

dados de desempenho de rede, suas limitações quanto à gestão de configuração e *backup* podem exigir soluções complementares para um gerenciamento completo de redes de computadores.

4.3.2. COMPORTAMENTOS OBSERVADOS: CACTI

Durante os testes realizados com o *Cacti*, foram observados diversos aspectos que afetam tanto a usabilidade quanto a eficácia da ferramenta. Apesar de a instalação da plataforma estar disponível em português, uma parte considerável dos termos permanece em inglês, o que pode confundir usuários que não dominam o idioma, especialmente em ambientes onde se espera uma total tradução. Essa falta de consistência na linguagem utilizada é um dos primeiros pontos negativos identificados.

Além disso, a interface do *Cacti* não se mostrou intuitiva, exigindo um conhecimento prévio ou consulta a fontes externas para a correta configuração e monitoramento de dispositivos. A necessidade de consultar a internet para realizar tarefas básicas, como a criação de monitoramento de dispositivos, demonstra que a ferramenta possui uma curva de aprendizado íngreme, o que pode ser um obstáculo para sua adoção em ambientes que demandam rapidez e eficiência.

Outro ponto relevante é a dependência do *Cacti* em relação à instalação de agentes específicos para que o monitoramento funcione de maneira adequada. Isso adiciona mais um nível de complexidade à sua implementação, pois exige que cada dispositivo a ser monitorado tenha o agente devidamente configurado e em funcionamento. Essa necessidade representa um desafio adicional para que todos os dispositivos da rede sejam monitorados.

Além dessas questões, foi observada a ausência de vários itens essenciais para a gestão eficiente de redes, como funcionalidades de *backup* e inventário. Essas ausências limitam a capacidade do *Cacti* de oferecer uma solução completa para a gestão de configuração de redes.

Em resumo, o *Cacti*, embora seja uma ferramenta robusta, apresenta dificuldades significativas que podem comprometer sua utilização eficiente na gestão de configuração de redes. A falta de uma tradução completa, a interface pouco intuitiva,

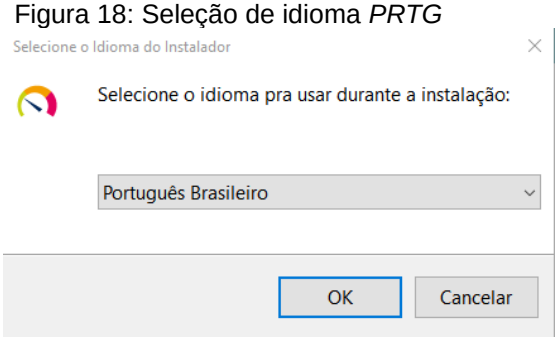
a necessidade de agentes adicionais e a ausência de funcionalidades essenciais como *backup* e inventário são pontos que desmotivam a sua utilização nos laboratórios de informática da UFES.

4.4. TESTE VIRTUAL: PRTG NETWORK MONITOR

O processo de instalação do *PRTG Network Monitor* foi realizado em etapas detalhadas para garantir uma experiência de configuração suave, mesmo para usuários com diferentes níveis de familiaridade com o *software*. A seguir, são apresentados os passos seguidos durante a instalação, incluindo detalhes de cada etapa e a importância de cada uma para o processo como um todo.

O primeiro passo foi o *download* do instalador do *PRTG Network Monitor* a partir do *site* oficial. O *PRTG* oferece uma versão de teste gratuita por 30 dias, permitindo que os usuários explorem as funcionalidades da ferramenta sem custo inicial. A documentação oficial, também disponível no *site*, foi utilizada para guiar o processo de instalação. Após iniciar o instalador, a primeira tela que surge permite ao usuário escolher o idioma que deseja utilizar durante a instalação e no uso posterior do *PRTG*. A seleção do idioma é essencial para garantir que todas as opções e comandos estejam claros e compreensíveis, adaptando o *software* às necessidades linguísticas do usuário. A Figura 18 representa essa configuração.

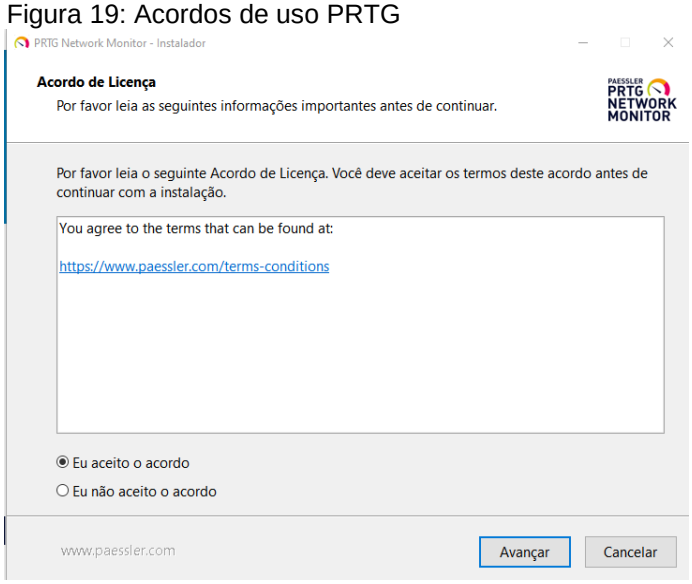
Figura 18: Seleção de idioma *PRTG*



Fonte: Autor

Em seguida, o instalador solicita que o usuário aceite os termos da licença do *software* (Figura 19). Este passo é crucial, pois estabelece o acordo legal entre o usuário e o fornecedor do PRTG. Após a leitura e aceitação dos termos, o processo de instalação pode prosseguir.

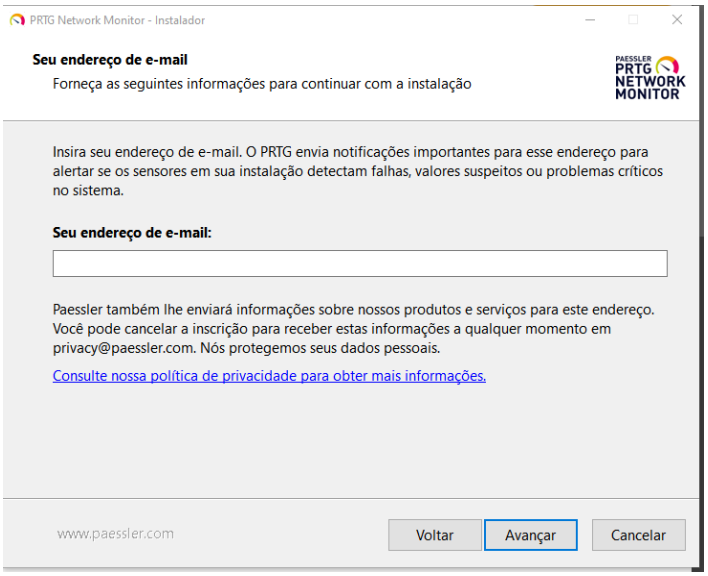
Figura 19: Acordos de uso PRTG



Fonte: Autor

O próximo passo envolve a inserção de um endereço de e-mail válido, como demostrado na Figura 20. Este e-mail é utilizado pelo *PRTG* para enviar informações importantes, como notificações de sistema e atualizações de software, além de ser necessário para a ativação da licença de teste.

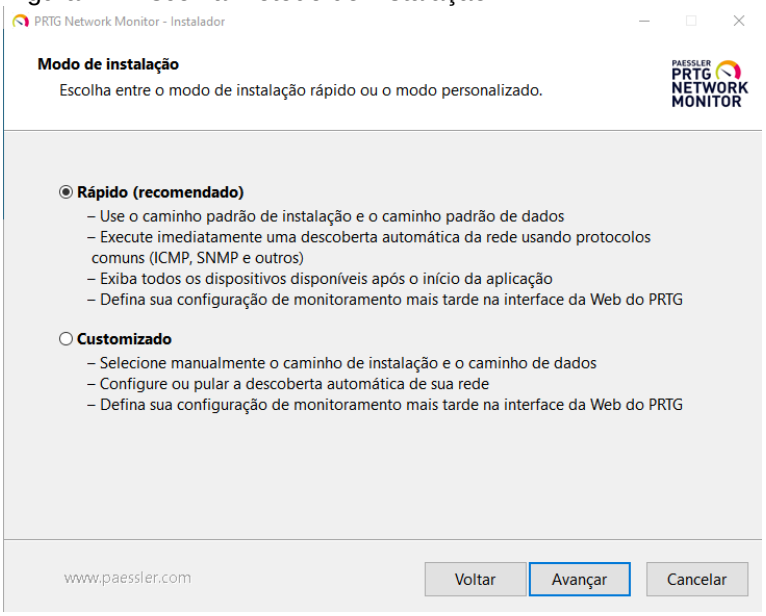
Figura 20: Endereço de *e-mail PRTG*



Fonte: Autor

O *PRTG* oferece diferentes modos de instalação, incluindo uma instalação recomendada que configura o sistema automaticamente para a maioria dos cenários de uso. Para este experimento, foi selecionado o modo de instalação recomendado, que irá atender satisfatoriamente a esse estudo, como demostrado na Figura 21.

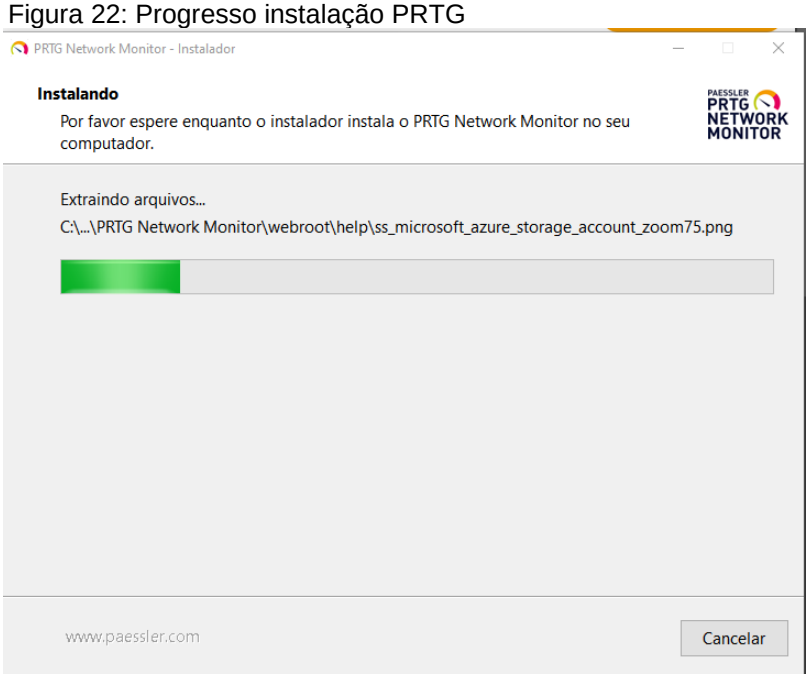
Figura 21: Escolha método de instalação



Fonte: Autor

Após a escolha do modo de instalação, o *software* começa a instalação propriamente dita, configurando todos os componentes necessários. Esta etapa pode levar alguns minutos, dependendo das especificações do sistema. Durante o processo, o instalador exibe uma barra de progresso, como podemos observar na Figura 22, permitindo ao usuário acompanhar a instalação em tempo real.

Figura 22: Progresso instalação PRTG

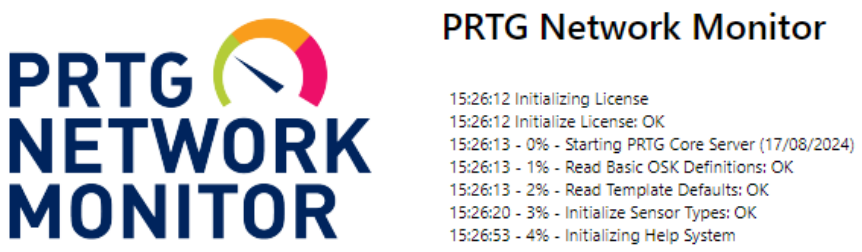


Fonte: Autor

Após a instalação, o *PRTG* inicia o servidor automaticamente. Durante este período, o software carrega todos os componentes necessários e prepara o ambiente para o

primeiro uso. (Figura 23) Esta etapa é crucial, pois garante que o sistema esteja operacional e pronto para ser utilizado.

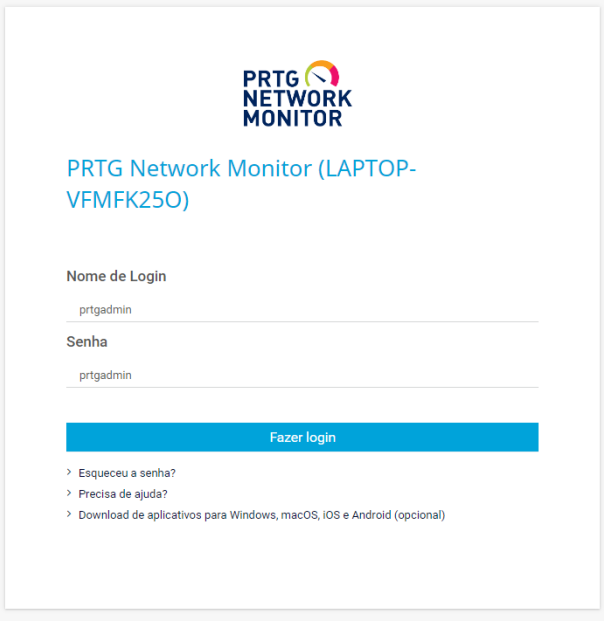
Figura 23: Carregamento do PRTG



Fonte: Autor

Uma vez que o servidor foi carregado, a tela de *login* do *PRTG* é exibida, como na Figura 24. Nesta tela, o usuário pode acessar o sistema utilizando as credenciais configuradas durante a instalação. O acesso ao painel de controle do *PRTG* marca o fim do processo de instalação e o início da configuração personalizada da ferramenta.

Figura 24: Tela de Login PRTG



Fonte: Autor

Ao acessar o sistema pela primeira vez, o *PRTG* realiza uma varredura inicial da rede, identificando automaticamente os dispositivos conectados. Esta funcionalidade demonstra a eficiência do *PRTG* em detectar e monitorar a infraestrutura de rede sem necessidade de configuração manual extensiva. A primeira tela (Figura 25) de

monitoramento já exibe os dispositivos encontrados, oferecendo uma visão imediata do estado da rede.

Figura 25: *Dashboard* PRTG

Fonte: Autor

A instalação do *PRTG Network Monitor* demonstrou ser um processo simples e intuitivo. Desde o *download* até a configuração inicial, cada etapa foi guiada de forma clara, com opções bem definidas que permitiram uma instalação tranquila, mesmo para usuários com pouca experiência em ferramentas de monitoramento de rede. A interface amigável e a configuração automatizada minimizam a complexidade técnica, permitindo que o *PRTG* esteja pronto para uso em questão de minutos. A capacidade do *software* de identificar automaticamente dispositivos na rede logo após a instalação reforça sua eficiência e utilidade.

4.4.1. PROCEDIMENTOS EXECUTADOS: PRTG NETWORK MONITOR

Durante a avaliação do *PRTG Network Monitor* em um ambiente de teste virtual, observou-se que a ferramenta oferece uma ampla gama de funcionalidades essenciais para a gestão de configuração de redes. Um dos recursos mais destacados é a descoberta automática de dispositivos, que permite ao *PRTG* realizar uma varredura na rede para identificar todos os dispositivos conectados, como *switches*, roteadores e servidores. Após a descoberta, o sistema sugere e configura automaticamente sensores adequados para cada dispositivo, como sensores de tráfego de rede, desempenho e disponibilidade, otimizando o processo de configuração e monitoramento.

A ferramenta também se destaca pela criação de mapas e painéis personalizados. Os mapas podem ser configurados para exibir a topologia da rede e o status dos dispositivos, enquanto os painéis personalizados fornecem visualizações detalhadas de gráficos de uso de largura de banda, histórico de desempenho e alertas em tempo real. Essas visualizações ajudam os administradores a monitorar a rede de forma intuitiva e a identificar problemas rapidamente.

O sistema de alertas do *PRTG* é altamente configurável, permitindo a criação de regras de notificação baseadas em condições específicas. Alertas sobre falhas de dispositivos, degradação de desempenho ou violações de limites críticos podem ser enviados por *e-mail, SMS* ou outras formas de comunicação, garantindo que a equipe de TI receba notificações prontamente. A funcionalidade de escalonamento de alertas é particularmente útil para gerenciar a gravidade dos problemas e a comunicação com diferentes membros da equipe conforme necessário.

O *PRTG* também oferece uma ferramenta robusta de relatórios que permite gerar relatórios detalhados sobre o desempenho e a saúde da rede. Esses relatórios incluem gráficos de desempenho, histórico de eventos e status dos dispositivos, facilitando a análise de tendências, auditorias e a apresentação de dados para a tomada de decisões. A capacidade de gerar relatórios personalizados e agendados suporta a análise contínua e a revisão periódica do desempenho da rede.

No que diz respeito ao monitoramento das configurações dos dispositivos, o *PRTG* permite verificar e auditar as configurações de roteadores, *switches* e outros equipamentos de rede. O rastreamento de mudanças nas configurações e a geração de alertas para alterações não autorizadas ajudam a assegurar que os dispositivos estejam configurados corretamente e conforme as políticas da organização.

Além disso, foi observado durante a experimentação que a ferramenta oferece opções de integração com outras ferramentas e sistemas de gestão de TI, incluindo sistemas de *ticketing* e ferramentas de automação. Essa capacidade de integração permite centralizar as operações e coordenar diferentes sistemas de gerenciamento. Embora o *PRTG* não execute *backups* diretamente, ele pode monitorar o *status* dos processos de *backup* e alertar sobre falhas ou problemas relacionados, contribuindo para a proteção e integridade dos dados.

Essas funcionalidades demonstram a eficácia do *PRTG Network Monitor* em proporcionar uma gestão abrangente e detalhada das configurações e do desempenho da rede, facilitando a manutenção proativa e a resposta rápida a incidentes.

4.4.2. COMPORTAMENTOS OBSERVADOS: PRTG NETWORK MONITOR

Durante o teste do *PRTG Network Monitor*, observou-se que a ferramenta se destacou pela facilidade e eficiência em vários aspectos críticos do gerenciamento de redes. A instalação do *PRTG* foi simples e direta, com um tempo total de apenas 20 minutos. A ferramenta apresentou uma interface gráfica amigável e clara, com suporte completo ao português, o que contribuiu para uma experiência de instalação sem erros de tradução. A configuração do sistema foi igualmente intuitiva, permitindo que sensores e dispositivos fossem configurados sem a necessidade de consultas adicionais à documentação.

A descoberta automática de dispositivos funcionou de maneira eficiente e satisfatória, permitindo a identificação e configuração rápida dos dispositivos na rede sem complicações. A facilidade de uso foi um ponto forte, com a ferramenta sendo altamente acessível e a interface gráfica oferecendo uma visualização clara e compreensível dos dados monitorados. A ausência de agentes de monitoramento nos dispositivos foi um aspecto positivo, simplificando ainda mais o processo de configuração.

No entanto, foi identificado que o *PRTG* não possui uma funcionalidade nativa de *backup* de dados, o que pode ser um ponto de atenção para a proteção e recuperação de dados críticos. Por outro lado, a ferramenta oferece uma série de integrações e um aplicativo nativo que permite o acesso remoto, ampliando a flexibilidade e a capacidade de gerenciamento.

Em resumo, o *PRTG Network Monitor* apresentou-se como uma solução de gerenciamento de redes eficiente e de fácil uso, com uma instalação rápida e uma configuração intuitiva. A integração de recursos e a interface amigável são aspectos

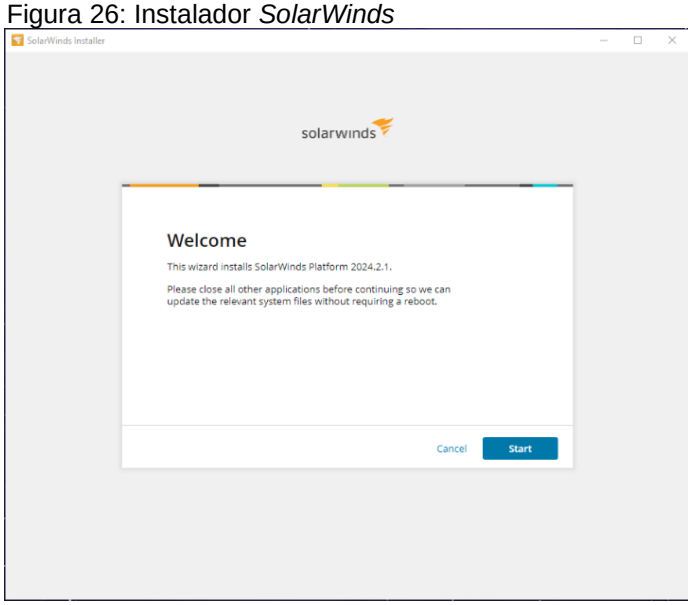
que contribuem para uma experiência de usuário positiva, apesar da limitação em termos de *backup*.

4.5. TESTE VIRTUAL: SOLARWINDS

O *SolarWinds Network Configuration Manager (NCM)* concluiu a primeira fase de testes de forma altamente eficaz, demonstrando ser uma solução robusta e confiável para o gerenciamento de redes. Disponível para os sistemas operacionais *Windows* e *Linux*, o *software* pode ser baixado diretamente do *site* oficial da *SolarWinds*. O *NCM* destaca-se por sua abrangência e pela eficácia com que aborda as complexidades do gerenciamento de redes, oferecendo uma vasta gama de recursos avançados que facilitam a administração e automação das tarefas de configuração de dispositivos de rede.

Após o preenchimento de um breve cadastro necessário para validar a licença de teste de trinta dias, o executável do *software* foi baixado e instalado na máquina de teste. A instalação foi realizada de maneira simples e intuitiva, permitindo que o ambiente de teste fosse configurado rapidamente para a exploração completa das funcionalidades do *NCM*. Na Figura 26, podemos observar a tela de inicialização do instalador, que fornece uma visão geral do processo de instalação.

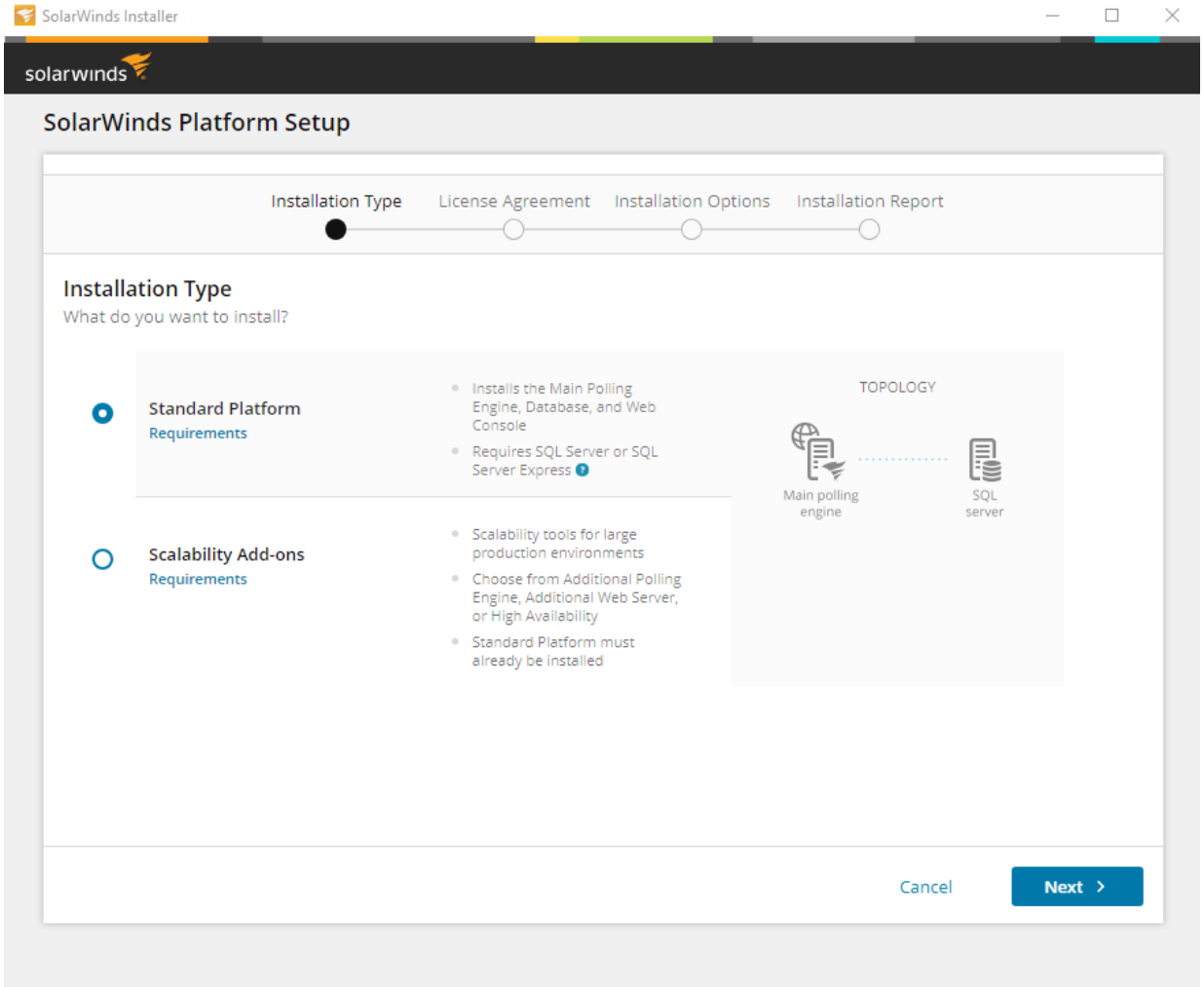
Figura 26: Instalador *SolarWinds*



Fonte: Autor

Para garantir a uniformidade dos testes com as demais ferramentas avaliadas, optou-se por seguir a instalação recomendada pela própria *SolarWinds*, conforme ilustrado na Figura 27. Esse procedimento assegura que todas as configurações estejam otimizadas para o desempenho do *software*, permitindo uma comparação justa entre as diferentes soluções testadas.

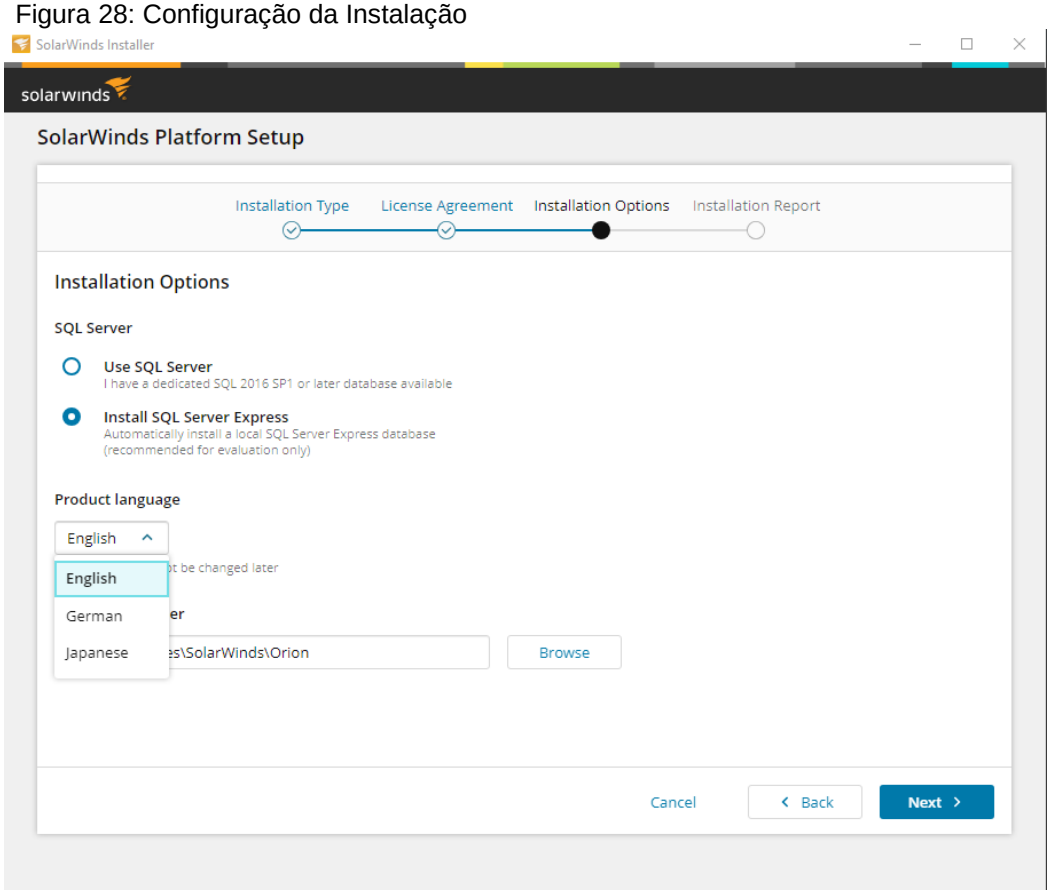
Figura 27: Método de instalação *SolarWinds*



Fonte: Autor

Na penúltima etapa da instalação, o usuário pode escolher o tipo de servidor de banco de dados a ser utilizado, uma decisão crucial para o desempenho e escalabilidade do *NCM*. Além disso, é possível selecionar o idioma da interface do *software*, que está disponível apenas em Inglês, Alemão e Japonês. A Figura 28 mostra esta etapa, onde também é definido o caminho em que o sistema será instalado no computador.

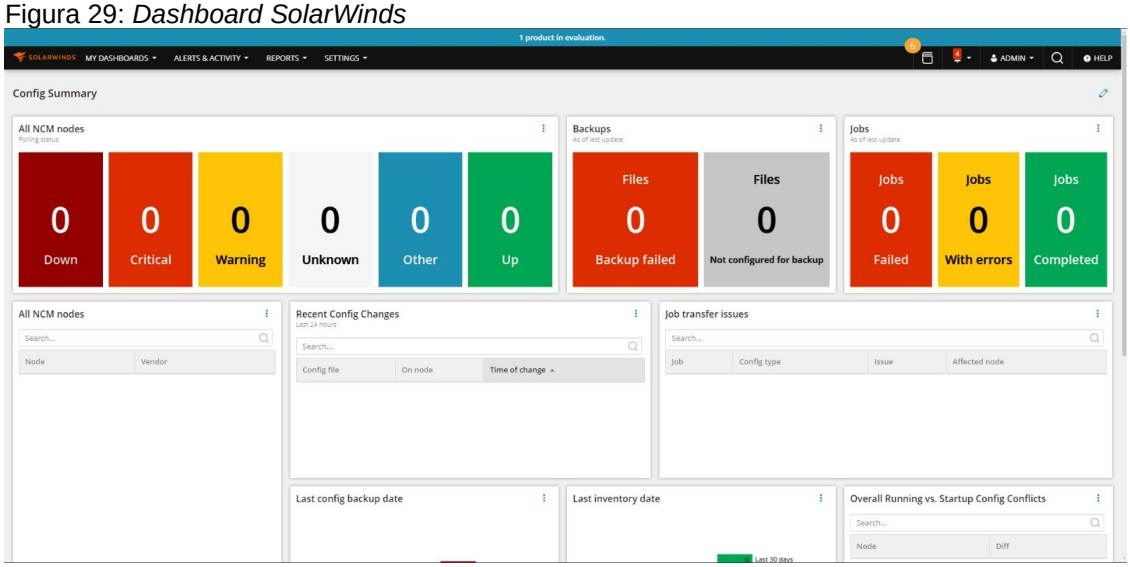
Figura 28: Configuração da Instalação



Fonte: Autor

Finalmente, antes de concluir a instalação, o instalador realiza uma verificação dos requisitos mínimos do sistema, garantindo que o computador em uso tenha a capacidade de executar o *SolarWinds NCM* de forma eficiente. Esta etapa é crucial para evitar problemas de desempenho. Assim terminado essa etapa já podemos visualizar o dashboard padrão do SolarWinds, demostrado na figura 29 abaixo.

Figura 29: *Dashboard SolarWinds*



Fonte: Autor

Esse processo de instalação detalhado reflete a atenção da *SolarWinds* em assegurar que o *NCM* seja configurado de forma adequada, proporcionando uma base sólida para seu funcionamento e para a realização dos testes subsequentes.

4.5.1. PROCEDIMENTOS EXECUTADOS: SOLARWINDS

Durante a fase de testes do *SolarWinds Network Configuration Manager (NCM),* foram executados diversos procedimentos para avaliar a funcionalidade e a eficácia do *software* em um ambiente controlado. Abaixo, apresentado as funcionalidades exploradas, os tipos de relatórios gerados, as telas observadas e os principais recursos oferecidos pela ferramenta.

***Backup* Automatizado de Rede:** Uma das funcionalidades mais importantes testadas foi o *backup* automatizado de configurações de dispositivos de rede, como roteadores e *switches*. O *NCM* permite a criação de tarefas agendadas para fazer *backup* regularmente das configurações, garantindo que as versões mais recentes estejam sempre disponíveis para restauração em caso de falhas ou mudanças indesejadas. Durante os testes, a configuração de *backups* automáticos foi realizada com sucesso, e os *backups* foram armazenados com versões anteriores disponíveis para comparação.

Gerenciamento de Configuração de *Switches*: O NCM oferece uma interface que facilita o gerenciamento centralizado de *switches*. Através dessa funcionalidade, foi possível visualizar tarefas como alterações de configuração em massa, aplicação de políticas de conformidade e verificação de mudanças. O software permite aplicar essas configurações de forma programada ou instantânea, o que foi testado e validado durante o uso.

Comparação de Configurações: Outro recurso essencial testado foi a capacidade de comparar configurações entre diferentes versões e dispositivos. Esta funcionalidade é útil para identificar mudanças que possam ter causado problemas na rede. O *SolarWinds NCM* foi capaz de detectar alterações nas configurações e apresentar relatórios detalhados sobre o que foi modificado, destacando as diferenças em um formato claro e compreensível.

Inventário de Rede: O *NCM* possui uma ferramenta robusta de inventário que foi utilizada para mapear todos os dispositivos de rede em teste. O *software* identificou e catalogou automaticamente os dispositivos, gerando um inventário detalhado. Este inventário inclui informações como versões de *firmware*, modelos de *hardware*, e outras especificações técnicas, permitindo uma visão abrangente da infraestrutura de rede.

Avaliação e Auditoria de Redes: As funcionalidades de avaliação e auditoria de rede foram exploradas para garantir a conformidade com políticas e normas de segurança. O *NCM* permite a criação de relatórios automatizados que documentam o estado atual da rede, as alterações realizadas e a conformidade com as políticas estabelecidas. Durante os testes, a ferramenta gerou relatórios de auditoria que foram revisados para garantir que todas as mudanças na configuração fossem documentadas e conformes às políticas de segurança da organização.

Automação de Configuração de Rede: A automação é uma das principais vantagens do *SolarWinds NCM*. Testes foram realizados para verificar a eficácia das ferramentas de automação em gerenciar alterações de configuração e garantir a conformidade. Através de *scripts* e *templates* pré-configurados, foi possível automatizar tarefas complexas e repetitivas, como a aplicação de atualizações de *firmware* ou a reconfiguração de dispositivos. Com a ferramenta é possível executar essas tarefas sem intervenção manual, demonstrando sua capacidade de reduzir o tempo e o esforço necessários para a manutenção da rede.

Gerenciamento de Mudanças e Configuração: A interface do *SolarWinds NCM* foi utilizada para gerenciar mudanças de configuração em vários dispositivos simultaneamente. O *software* oferece uma visão centralizada das mudanças realizadas, com alertas em tempo real sobre modificações não autorizadas ou falhas no processo de configuração. Durante os testes, foi percebido que as alterações realizadas fossem monitoradas e documentadas, proporcionando uma trilha de auditoria clara e confiável.

Relatórios e *Dashboards*: O *NCM* inclui uma série de relatórios pré-configurados e a capacidade de criar relatórios personalizados. Esses relatórios abrangem uma variedade de métricas e informações, como status de conformidade, históricos de

backup, e detalhes de inventário. Além dos relatórios, o *software* oferece *dashboards* personalizáveis, onde os administradores podem visualizar rapidamente o estado da rede e identificar possíveis problemas.

Esses procedimentos permitiram uma avaliação abrangente do *SolarWinds Network Configuration Manager*, demonstrando sua capacidade de atender às necessidades de gerenciamento de configuração, inventário, e automação em um ambiente de rede de computadores mais exigente. O *SOLARWINDS* não apenas otimiza a gestão de múltiplos dispositivos, mas também garante a segurança e a conformidade de cada um deles, proporcionando uma abordagem integrada e confiável para monitoramento e controle.

4.5.2. COMPORTAMENTOS OBSERVADOS: SOLARWINDS

Durante a exploração do *SolarWinds Network Configuration Manager (NCM),* foram observadas várias funcionalidades avançadas que o diferenciam das demais ferramentas testadas. O *SolarWinds NCM* se destacou principalmente pela robustez de suas ferramentas de gerenciamento de configuração, oferecendo um conjunto completo de funcionalidades para *backup* automatizado de configurações, gerenciamento centralizado de alterações, e auditorias detalhadas de conformidade.

Uma das principais vantagens do *SolarWinds NCM* é a capacidade de realizar *backups* automáticos das configurações de dispositivos de rede, o que não é nativamente suportado pelas outras ferramentas. Além disso, o *software* permite comparar versões de configurações de roteadores e *switches*, identificando rapidamente quaisquer alterações e ajudando a rastrear a origem de problemas de rede. Esse nível de detalhamento e controle sobre as configurações de rede é algo que faltou nas outras ferramentas testadas.

Outra funcionalidade única do *SolarWinds* é a automação de tarefas de configuração, que economiza tempo e reduz o risco de erros humanos, um recurso não disponível de maneira tão abrangente no *Zabbix*, *PRTG* ou *CACTI*. Além disso, a ferramenta oferece uma integração sólida com uma variedade de dispositivos de rede de múltiplos fornecedores, algo que facilita a gestão de ambientes heterogêneos.

A capacidade do *SolarWinds NCM* de realizar auditorias de rede e gerar relatórios detalhados sobre o estado da infraestrutura de rede também supera as capacidades das outras ferramentas, que são mais focadas no monitoramento de desempenho do que no gerenciamento de configuração e conformidade. Enquanto o *Zabbix* e o *PRTG* oferecem monitoramento eficaz e são adequados para acompanhar a performance da rede em tempo real, eles não possuem a mesma profundidade nas funcionalidades de gestão de configuração.

O *SolarWinds Network Configuration Manager (NCM)* demonstrou ser uma solução excepcional no contexto de gerenciamento de configuração de redes, destacando-se entre as ferramentas testadas. Suas funcionalidades avançadas, como *backup* automatizado, gerenciamento centralizado de alterações e auditorias detalhadas de conformidade, oferecem um controle rigoroso e uma gestão eficaz da infraestrutura de rede. Comparado ao *Zabbix*, *PRTG Network Monitor e CACTI*, o *SolarWinds NCM* não só provou ser mais robusto na automação de tarefas e no gerenciamento de múltiplos dispositivos, mas também se mostrou superior em termos de segurança, graças à sua capacidade de verificar e corrigir vulnerabilidades de rede.

4.6. RESULTADOS DO TESTE VIRTUAL

Nesta seção, serão apresentados os resultados obtidos após a realização dos testes virtuais com as quatro ferramentas selecionadas para o gerenciamento de configuração de redes*: Zabbix, PRTG Network Monitor, CACTI e SolarWinds Network Configuration Manager (NCM).* A avaliação foi conduzida com base nos critérios estabelecidos na metodologia, permitindo uma análise comparativa entre as soluções.

Os testes realizados demonstraram que cada ferramenta possui características distintas que podem atender a diferentes necessidades de gestão de configuração de redes. O *Zabbix* se destacou pela robustez na coleta de dados de desempenho e monitoramento contínuo, embora sua configuração inicial tenha sido mais complexa e demandado maior familiaridade com sistemas *Linux*. Já o *PRTG Network Monitor* apresentou uma instalação simples e intuitiva, com uma interface gráfica amigável e suporte nativo em português, mas sua funcionalidade de *backup* foi limitada, restringindo-se ao monitoramento.

O *CACTI*, por sua vez, apresentou-se como uma solução intermediária, combinando monitoramento com a geração de gráficos detalhados, mas exigindo configurações mais avançadas para alcançar resultados otimizados. Por fim, o *SolarWinds NCM* foi avaliado como uma ferramenta altamente eficiente e abrangente, com funcionalidades robustas para backup, auditoria e gerenciamento de dispositivos de rede, embora sua interface e recursos estejam mais orientados para usuários experientes.

Os resultados detalhados de cada ferramenta, conforme os critérios de avaliação adotados, podem ser consultados na Tabela 3, a seguir. Essa análise permitirá uma melhor escolha da ferramenta mais adequada para o gerenciamento de configuração de redes nos laboratórios de informática da UFES. Atualmente, os laboratórios não possuem nenhum tipo de monitoramento, o que representa um desafio significativo, considerando que há mais de 200 computadores distribuídos em dois prédios distantes no campus, sem a utilização de switches gerenciáveis.

Tabela 3 - Resultados Comparativo Teste Virtual

Ferramenta	**ZABBIX**	**CACTI**	**PRTG**	**SOLARWINDS**
Grau de Dificuldade da Instalação	**4**	**5**	**1**	**2**
Tempo (minutos)	**240**	**>1000**	**20**	**40**
Descoberta Automática	Ausente, necessita de uso de agente	Ausente, necessita de uso de agente	Presente	Presente
Configuração	Moderada	Difícil	Fácil	Fácil
Grau de Dificuldade	3	5	1	1
Interface Gráfica	3	5	1	2
Nível de Acesso à Informação	1	5	2	2
Impressões	O gerente só pode ser instalado em Linux. Possui vasta documentação oficial	Não atende aos requisitos para gestão de configurações de redes	Fácil instalação e configuração. Interface bem intuitiva	Interface intuitiva, mas requer atenção por não possuir tradução

Fonte: Autor

Observa-se que o *PRTG* se destaca pela facilidade de instalação, com o menor tempo necessário, enquanto o *Cacti* apresenta a maior dificuldade, exigindo um nível elevado de conhecimento técnico e um longo tempo de configuração. O *SolarWinds* e o *Zabbix* também apresentam um tempo de instalação relativamente longo, mas consideravelmente menor que o do *Cacti*. Em termos de descoberta automática de dispositivos, o *PRTG* e o *SolarWinds* se destacam por oferecerem essa funcionalidade de forma eficiente, ao passo que o *Zabbix* e o *Cacti* requerem a instalação de agentes específicos, aumentando a complexidade do processo de configuração e monitoramento.

No que diz respeito à facilidade de configuração e à qualidade da interface gráfica, o *PRTG* sobressai como a ferramenta mais intuitiva e fácil de configurar. O *SolarWinds* também oferece uma interface gráfica de boa qualidade, embora exija maior atenção devido à falta de tradução completa. O *Cacti*, por sua vez, é classificado como a mais difícil de configurar e com a interface menos intuitiva. Quanto ao nível de acesso à informação, o *Zabbix* oferece a maior profundidade, mas com uma interface difícil de utilizar, seguido pelo *SolarWinds* e *PRTG*. O *Cacti*, por outro lado, apresenta o menor nível de acesso à informação.

As impressões gerais destacam a adequação e as limitações de cada ferramenta. O *Zabbix*, apesar das dificuldades de instalação, é robusto e possui vasta documentação oficial, embora seja limitado à instalação em sistemas *Linux*. O *Cacti*, no entanto, não satisfaz os requisitos para a gestão de configurações de redes devido à ausência de alguns componentes nativos. Já o *PRTG* se sobressai pela instalação e configuração simples, além de uma interface intuitiva. O *SolarWinds* também é bem avaliado, embora a falta de tradução completa possa gerar dificuldades adicionais.

Dentre os testes realizados, as ferramentas que mais se destacam são o *Zabbix* e o *PRTG*, que avançam para os testes físicos, uma vez que oferecem um bom equilíbrio entre funcionalidade, usabilidade e facilidade de configuração, sendo as opções mais promissoras para atender às necessidades específicas dos laboratórios de informática da UFES.

4.7. TESTE FÍSICO

Esta sessão dedica-se à realização dos testes físicos das ferramentas selecionadas com base na análise preliminar em ambiente virtual. Este estágio do estudo objetiva avaliar a aplicabilidade e a eficácia das ferramentas *Zabbix* e *SolarWinds* em um ambiente real, onde são considerados os desafios e variáveis inerentes às redes operacionais. A execução dos testes físicos visa corroborar a capacidade dessas soluções em atender às exigências específicas de monitoramento e gestão de configuração de redes nos laboratórios de informática da Universidade Federal do Espírito Santo (UFES). Para tanto, serão realizadas as etapas de instalação, configuração e operação das ferramentas em um ambiente controlado, com o propósito de avaliar sua performance, usabilidade e impacto na infraestrutura existente, fornecendo uma análise detalhada e conclusiva sobre sua adequação ao contexto proposto.

4.7.1. PREPARAÇÃO DO AMBIENTE

O teste físico será realizado no Laboratório de Desenvolvimento de Software 2 (Lab 06), localizado no Reuni da UFES. Este laboratório é composto por 20 computadores, todos configurados para acesso à internet e integrados por meio de um switch de marca Tenda, modelo TEG1024D. O switch oferece suporte a conexões gigabit, assegurando uma alta taxa de transferência de dados, essencial para testes de rede e monitoramento em tempo real. A infraestrutura do laboratório é conectada ao Centro de Processamento de Dados (CPD) da STI-Sul através de um cabo de fibra óptica, o que garante latência mínima e um ambiente de rede mais robusto para as avaliações.

Esta configuração permite que os testes simulem situações reais de gestão e monitoramento de redes em um ambiente controlado, refletindo a infraestrutura de TI encontrada em organizações de médio a grande porte. Na figura 30 podemos observar a disposição do laboratório e seus recursos.

Figura 30: Laboratório de Desenvolvimento de *Software* 2

Fonte: Autor

Inicialmente, a ferramenta *Zabbix* será testada. Para isso, será aproveitada a configuração já realizada durante o teste virtual, com ajustes necessários para integrar o ambiente de rede específico do laboratório. Em seguida, será feito o mesmo procedimento para a ferramenta *SolarWinds*, mantendo a continuidade do ambiente previamente configurado.

O processo de teste será conduzido da seguinte forma: dos 20 computadores, um permanecerá desligado para fins de teste. O servidor será ligado e as configurações necessárias serão aplicadas para garantir a comunicação com a rede do laboratório. Em seguida, será realizada a inclusão do computador que estava desligado, permitindo a monitoração do processo de detecção automática e inclusão de dispositivos na rede.

A partir desse ponto, serão conduzidas diversas operações, como o inventário da rede, a geração de gráficos de desempenho e a configuração de *backups* das configurações do sistema. Serão criados *scripts* específicos para monitoramento e

alerta de problemas de configuração, além de configurar alertas que sejam acionados em situações críticas. Por fim, será realizada a atualização das configurações de rede, garantindo que a ferramenta esteja apta a gerenciar eventuais alterações no ambiente de maneira eficaz e precisa, assegurando a integridade da infraestrutura de rede e a continuidade dos serviços fornecidos pelo laboratório.

4.7.2. TESTE FÍSICO: ZABBIX

Para a execução dos testes utilizando o *Zabbix*, foi necessário realizar a instalação do agente *Zabbix* em cada dispositivo que seria monitorado. O processo de instalação do agente, amplamente compatível com diversos sistemas operacionais, demonstrou-se simples e direto, exigindo apenas o cumprimento de etapas padronizadas. Inicialmente, efetuou-se o download do agente específico para cada sistema e, em seguida, configurou-se o direcionamento adequado para o *IP* do servidor *Zabbix*, que no cenário de teste correspondia ao endereço 192.168.36.91. Também foi necessário especificar a porta de comunicação 10050, padrão para a interação entre o agente e o servidor.

Após a instalação do agente em cada máquina, validou-se o *status* do serviço nos dispositivos com sistema operacional *Windows*, assegurando-se de que o agente estivesse corretamente ativo. Adicionalmente, verificou-se a configuração dos *firewalls* em cada computador, garantindo que a porta 10050 estivesse liberada para permitir o tráfego de dados entre o agente e o servidor *Zabbix*.

Como a regra de descoberta de rede já havia sido configurada durante os testes virtuais, o *Zabbix* automaticamente detectou e inseriu os novos *hosts* no seu sistema de monitoramento no teste físico. Esse processo automatizado facilitou a identificação rápida dos dispositivos conectados à rede, sem a necessidade de configuração manual para cada novo *host*. Na Figura 31, é apresentada a tela com todos os *hosts* monitorados pelo *software*, destacando-se os dispositivos localizados no Laboratório de Desenvolvimento de Software 2. Embora o *Zabbix* tenha identificado outros dispositivos na rede, esses foram desconsiderados, visto que o foco do teste estava nos equipamentos do laboratório. Na tela apresentada, os principais campos visíveis incluem: Nome, que identifica cada dispositivo monitorado; Interface, que indica o

endereço de rede associado ao dispositivo; Disponibilidade, que demonstra o status atual do dispositivo (*online* ou *offline*); Etiquetas, usadas para categorizar e organizar os dispositivos de forma eficiente; *Status*, que exibe a condição atual do equipamento; Dados Recentes, que apresenta informações coletadas em tempo real sobre o desempenho; Incidentes, que detalha quaisquer problemas ou alertas detectados; e Gráficos/*Dashboards*, que fornecem uma visualização gráfica do desempenho e métricas do dispositivo ao longo do tempo.

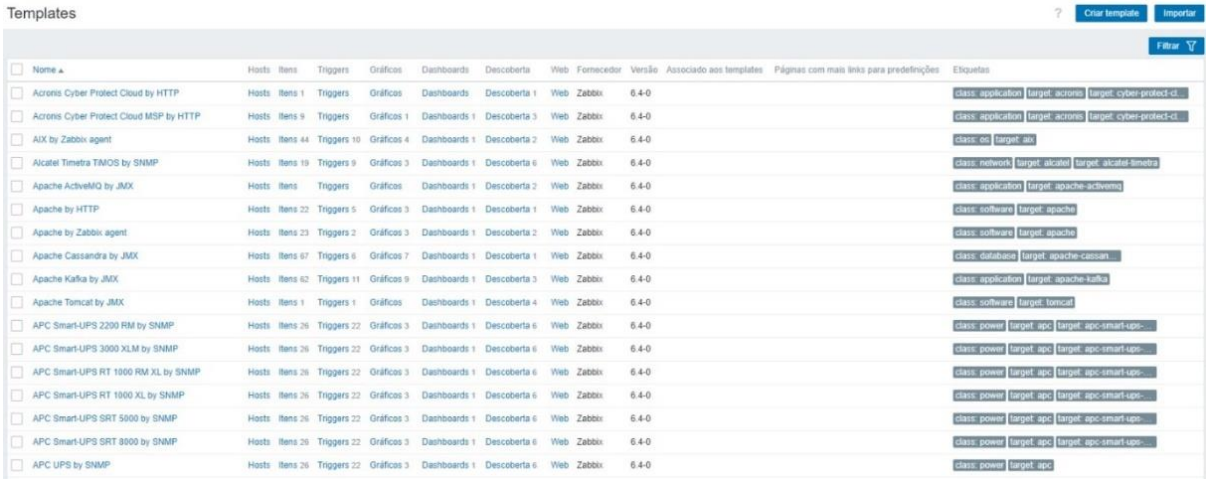
Figura 31: Interface de monitoramento de *Hosts*

Fonte: Autor

Para configurar a regra de descoberta no *Zabbix*, o processo iniciou-se acessando o menu de "Configuração" e selecionando "Descoberta de Rede". Em seguida, foi criada uma nova regra de descoberta ao clicar em "Criar Regra de Descoberta". Nessa etapa, foi fornecido um nome descritivo para a regra, como "Descoberta de Dispositivos do Laboratório", e definido o intervalo de tempo em que a descoberta seria realizada. O intervalo de *IPs* a ser escaneado também foi especificado, abrangendo a rede do laboratório, como "192.168.36.1-192.168.36.254". Além disso, foram configuradas condições de descoberta, como resposta o "Agente Zabbix", para garantir que apenas dispositivos específicos fossem detectados. Na seção de ações, foram definidas as tarefas que o *Zabbix* executaria ao encontrar um novo *host*, como adicioná-lo automaticamente ao monitoramento, associá-lo a *templates* específicos (como templates para *Windows* ou *Linux*) e enviar notificações. Após salvar a regra, o *Zabbix* realizava a descoberta conforme o intervalo estabelecido, inserindo novos *hosts* automaticamente de acordo com as ações predefinidas.

Durante a configuração dos dispositivos no *Zabbix*, não foi necessário criar novos *templates*, uma vez que a ferramenta já oferece uma ampla variedade de *templates* predefinidos. Esses *templates* são modelos de monitoramento que contêm todas as métricas, itens e *triggers* necessários para coletar dados de sistemas e dispositivos específicos, como servidores *Linux*, *Windows*, roteadores, *switches* e outros equipamentos de rede. No teste, foram utilizados templates já instalados, como o "*Template OS Linux*" e *"Template OS Windows",* que possibilitaram a rápida associação dos dispositivos ao sistema de monitoramento. Esses *templates* predefinidos reduziram o tempo de configuração e garantiram que os parâmetros corretos fossem monitorados automaticamente, como o uso de *CPU*, memória, disponibilidade de disco, e serviços ativos. A utilização desses *templates* facilitou significativamente o processo de monitoramento, permitindo uma abordagem padronizada e eficaz sem a necessidade de configurações manuais adicionais. Na Figura 32 podemos observar alguns desses *templates*, bem como podemos editá-los, importar *templates* e criar novos *templates* conforme nescessario.

Figura 32: *Templates* do *Zabbix*

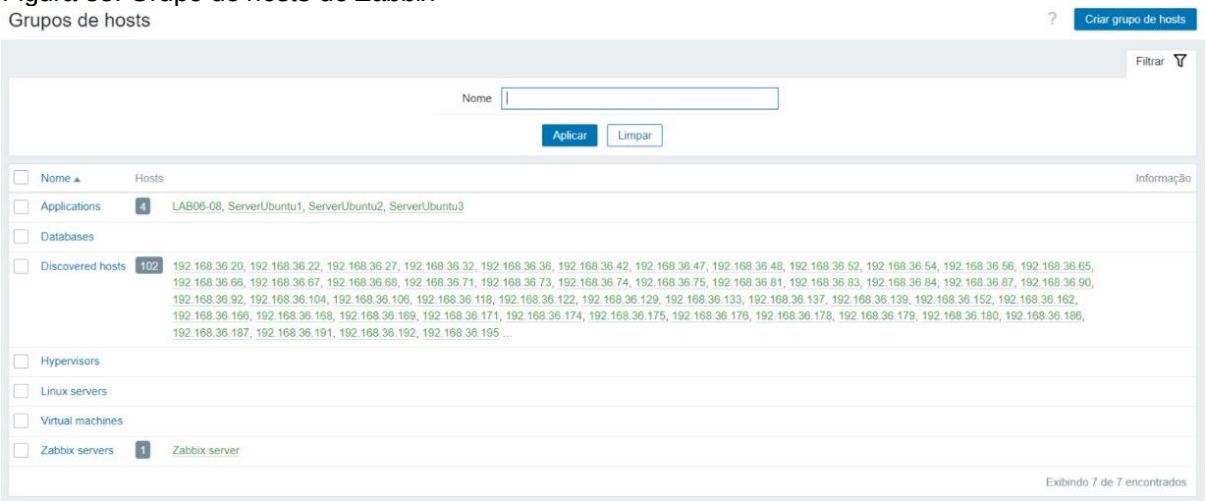


Fonte: Autor

No *Zabbix*, o conceito de "Grupo de *Hosts*" refere-se à organização lógica dos dispositivos monitorados, permitindo que eles sejam agrupados de acordo com critérios específicos, como função, localização ou tipo de equipamento. Essa funcionalidade é extremamente útil para ambientes como os laboratórios de informática da UFES, pois facilita a gestão e visualização dos dispositivos de forma estruturada e eficiente. Na Figura 33, observa-se a organização padrão do *Zabbix*, foi configurado que os novos *Hosts* fossem inseridos no grupo de descobertas e os servidores *Linux* foram alocados na parte de aplicações.

Ao utilizar grupos de *hosts*, a administração pode aplicar regras de monitoramento, gráficos e *templates* de forma coletiva, agilizando processos e reduzindo o trabalho manual. Além disso, é possível gerar relatórios e criar alertas personalizados para um grupo inteiro de dispositivos, o que torna a gestão de laboratórios mais eficiente, especialmente quando há uma grande quantidade de equipamentos conectados à rede. Isso também facilita a criação de políticas de *backup* e atualização de configurações, centralizando as ações em um único grupo e garantindo que todos os dispositivos sigam os mesmos parâmetros de segurança e desempenho.

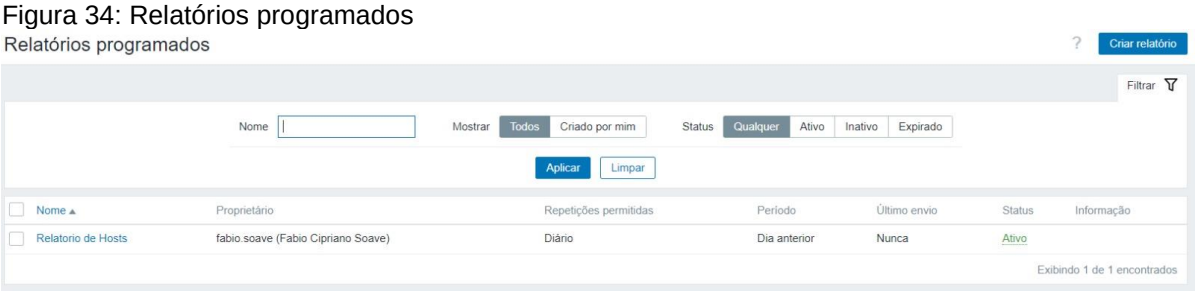
Figura 33: Grupo de *hosts* do *Zabbix*



Fonte: Autor

Os relatórios no *Zabbix* oferecem uma visão detalhada e organizada das métricas e dados coletados dos dispositivos monitorados. Eles permitem a análise do desempenho de *hosts*, serviços e redes ao longo do tempo, o que auxilia na tomada de decisões e no planejamento de melhorias. Na Figura 34, por exemplo, é apresentado um relatório programado de *hosts* com informações dos dispositivos no Laboratório de Desenvolvimento de *Software* 2. Esse relatório compila informações como tempo de atividade e incidentes registrados, fornecendo um visão sobre os dispositivos e sua operação no dia anterior.

Figura 34: Relatórios programados



Fonte: Autor

Os relatórios podem ser configurados para serem gerados automaticamente em intervalos regulares ou sob demanda, o que facilita a monitoração contínua sem intervenção manual constante. É possível customizar os tipos de relatórios de acordo com as necessidades específicas, seja para analisar problemas de desempenho ou para verificar a eficácia de medidas de segurança e *backup*. Esses relatórios são úteis não apenas para o diagnóstico de problemas, mas também para auditorias e conformidades, proporcionando uma documentação completa das atividades de monitoramento. Com essa funcionalidade, a equipe de TI pode identificar tendências, prever falhas e implementar melhorias antes que ocorram incidentes críticos, garantindo maior estabilidade na rede do laboratório.

Durante a configuração do *Zabbix* nos testes realizados, foram implementadas rotinas de *backup* para garantir a segurança dos dados monitorados. O processo de *backup* foi realizado utilizando o *mysqldump* para capturar todas as informações armazenadas no banco de dados *MySQL*, onde estão registrados os *hosts*, métricas, eventos e alertas. Além disso, foi efetuado o *backup* dos arquivos de configuração do *Zabbix*, que contêm dados cruciais, como *templates*, grupos de *hosts*, permissões de usuários e configurações específicas da rede monitorada.

Os *backups* foram programados para ocorrer de forma automatizada, utilizando *cron jobs* no servidor, com uma frequência diária para assegurar a integridade dos dados em caso de falhas ou incidentes. Essa rotina permitiu que o ambiente de monitoramento estivesse sempre protegido, e que, em eventual necessidade, os dados pudessem ser restaurados de maneira eficiente.

Figura 35: *Log* de auditoria

Log de auditoria

Reduzir o zoom | Última 1 hora | Filtrar

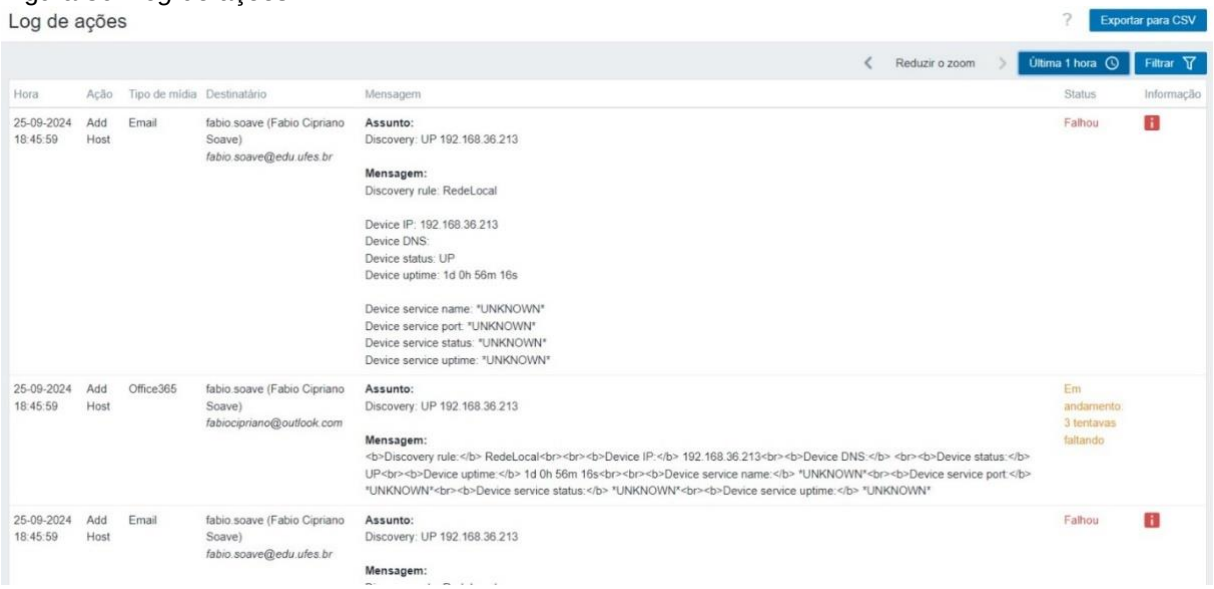
Hora	Usuário	IP	Recurso	ID	Ação	ID do conjunto de registros	Detalhes	
25-09-2024 18:37:22	*System*		Host	10728	Adicionar	cm1idyt6k00v22k038x6sw2u7	Descrição: 192.168.36.126 host.groups[744]: Adicionado host.groups[744].groupid: 5	Detalhes
25-09-2024 18:31:16	Admin	192.168.36.64	Mapa	2	Adicionar	cm1idqyi40000b603qzk1zake	Descrição: TesteReal	
25-09-2024 18:24:10	*System*		Host	10727	Adicionar	cm1idhtkc00043303tbak9e7v	Descrição: LAB06-19 host.groups[743]: Adicionado host.groups[743].groupid: 5	Detalhes
25-09-2024 18:22:37	*System*		Host	10726	Adicionar	cm1idftr800063103yymp8xku	Descrição: LAB07-18 host.groups[742]: Adicionado host.groups[742].groupid: 5	Detalhes
25-09-2024 18:06:42	*System*		Host	10725	Adicionar	cm1icvdkh00042z03tbak9e7v	Descrição: LAB06-04 host.groups[741]: Adicionado host.groups[741].groupid: 5	Detalhes
25-09-2024 18:04:06	*System*		Trigger	23945	Adicionar	cm1ics0t900lj2f03dx1dyrz1	Descrição: "webthreatdefusersvc_1b2624d" (Serviço de Defesa do Usuário Contra Ameaças da Web_1b2624d) is not running trigger: Adicionado	Detalhes

Fonte: Autor

Durante os testes realizados, foi explorada a funcionalidade do *Log* de Auditoria, como ilustrado na Figura 35. O *Log* de Auditoria permitiu o registro detalhado de todas as atividades administrativas no sistema *Zabbix*, como alterações nas configurações, adição ou remoção de *hosts*, e modificações nas permissões de usuários. Esse recurso foi fundamental para acompanhar o histórico de ações realizadas pelos administradores, oferecendo uma visão clara de quem alterou o quê e quando, garantindo uma maior segurança e controle no ambiente de monitoramento. Esse nível de rastreabilidade facilita a identificação de problemas ou alterações indevidas, sendo uma ferramenta indispensável para ambientes como os laboratórios de informática da UFES.

Além do *Log* de Auditoria, também foi utilizado o *Log* de Ações (Figura 36), que registrou as atividades automatizadas executadas pelo sistema em resposta a eventos de monitoramento. O *Log* de Ações armazenou dados sobre disparos de alertas, notificações enviadas aos administradores, execuções de *scripts* automatizados, e outros tipos de respostas automáticas configuradas no *Zabbix*. Essa funcionalidade foi essencial para verificar se os alertas e notificações programadas estavam funcionando corretamente, além de permitir uma análise detalhada das reações do sistema frente a falhas ou alterações na rede monitorada.

Figura 36: *Log* de ações

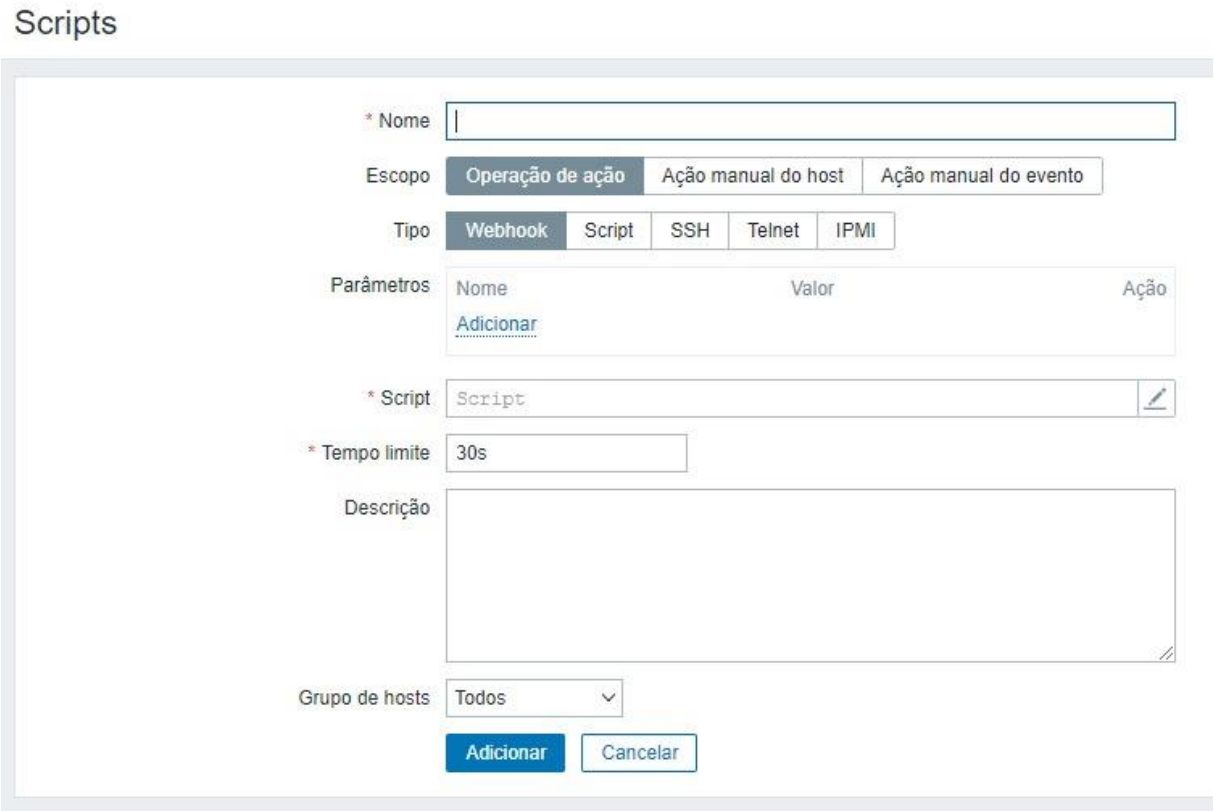


Fonte: Autor

Na Figura 37, foi explorada a funcionalidade de execução de *scripts* no *Zabbix*, um recurso que permite a automação de tarefas de gerenciamento diretamente a partir da interface da ferramenta. Os *scripts* configurados possibilitam a execução remota de comandos em *hosts* monitorados, sem a necessidade de acesso físico ou manual aos dispositivos. Esse recurso pode ser utilizado para realizar verificações rápidas em dispositivos, como *ping* e diagnósticos básicos de conectividade, além de reinicializações de serviços de rede.

A configuração dos *scripts* no *Zabbix* é relativamente simples, bastando definir o comando a ser executado e vinculá-lo a um grupo de *hosts* ou a um *host* específico. Isso possibilita uma resposta rápida a eventos detectados pelo sistema, como a reinicialização de serviços de rede em caso de falhas. A flexibilidade oferecida pela execução de *scripts* trouxe uma vantagem significativa, permitindo a automação de processos rotineiros e a intervenção imediata em dispositivos, quando necessário, aumentando a eficiência na administração do ambiente dos laboratórios da UFES.

Figura 37: *Scripts* personalizáveis



Fonte: Autor

No *Zabbix*, as Ações são um recurso avançado que permite automatizar respostas e notificações com base em eventos detectados pelo sistema de monitoramento. Durante os testes, foi explorada a capacidade de configurar Ações para responder a diferentes situações, como a identificação de novos *hosts*, a falha em um serviço ou a indisponibilidade de um dispositivo.

As Ações no Zabbix podem ser configuradas para executar uma série de tarefas, como enviar notificações por e-mail, executar *scripts* personalizados, enviar mensagens para sistemas de mensageria instantânea, ou até mesmo reiniciar serviços. A configuração de Ações é altamente flexível, permitindo definir condições específicas para sua execução. Por exemplo, foi criada uma ação para enviar um alerta por e-mail sempre que o Zabbix detectava um novo *host*.

Essas Ações automatizadas facilitam a resposta imediata a problemas na rede, permitindo que os administradores sejam notificados ou que o próprio sistema tente corrigir o problema automaticamente, sem a necessidade de intervenção manual imediata. Na Figura 38, vemos quais ações podem ser configuradas.

Figura 38: Menu de Alertas

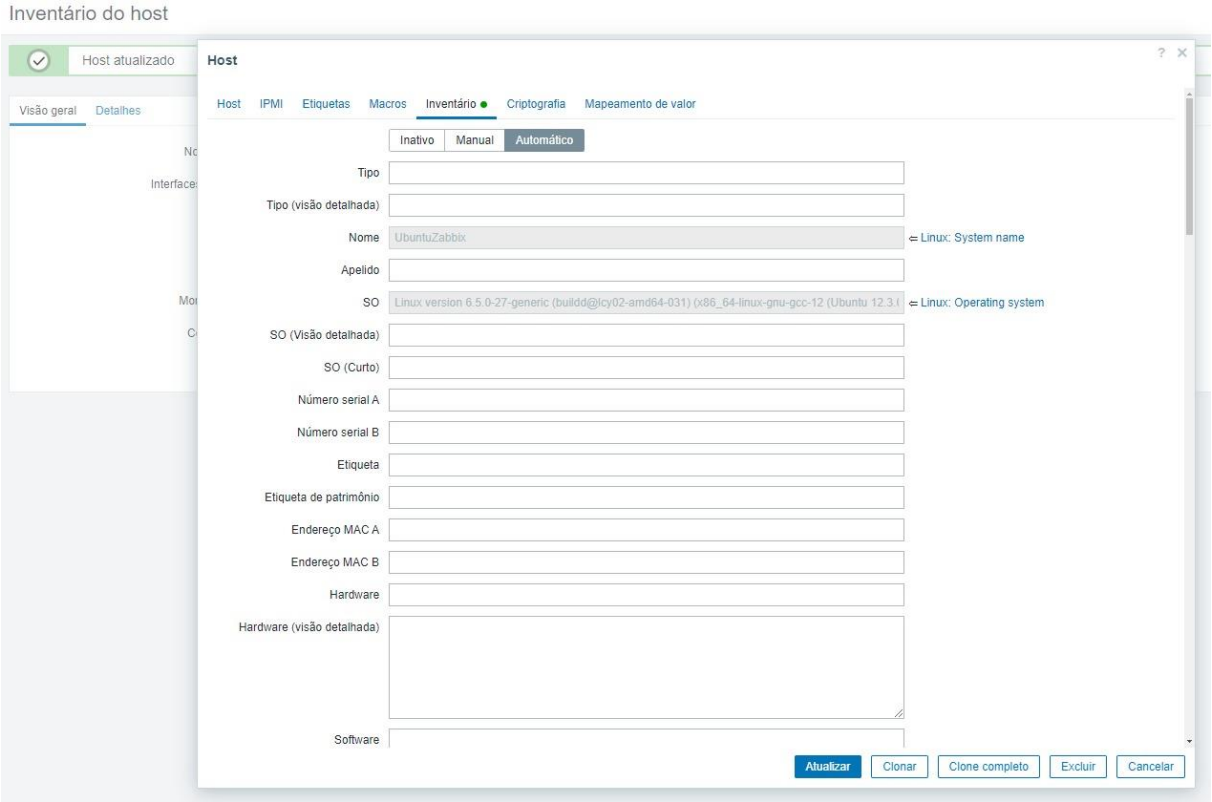
Fonte: Autor

No Zabbix, o Inventário do Host é uma funcionalidade essencial para a organização e gerenciamento dos dispositivos monitorados. Ao ser explorado durante os testes, o inventário revelou-se uma ferramenta útil para armazenar e visualizar informações detalhadas de cada host, como nome, endereço IP, localização física, responsável pela máquina, sistema operacional, e outros atributos configuráveis.

A Figura 39 ilustra como o *Zabbix* exibe essas informações de maneira organizada. O inventário pode ser preenchido de forma automática, conforme o *Zabbix* coleta dados dos *hosts*, ou manualmente, permitindo que o administrador insira detalhes específicos conforme necessário. Cada *host* monitorado pode ter seu inventário habilitado para coletar informações adicionais, como número de série do *hardware*, versão do *software*, entre outros dados importantes para a gestão da rede.

Essa funcionalidade permite, por exemplo, que o administrador tenha uma visão clara de todos os equipamentos conectados à rede, facilitando a criação de relatórios detalhados e a manutenção de um registro atualizado dos ativos de TI. Além disso, o inventário pode ser utilizado em conjunto com alertas e *scripts*, aprimorando a automação das tarefas de monitoramento e gerenciamento.

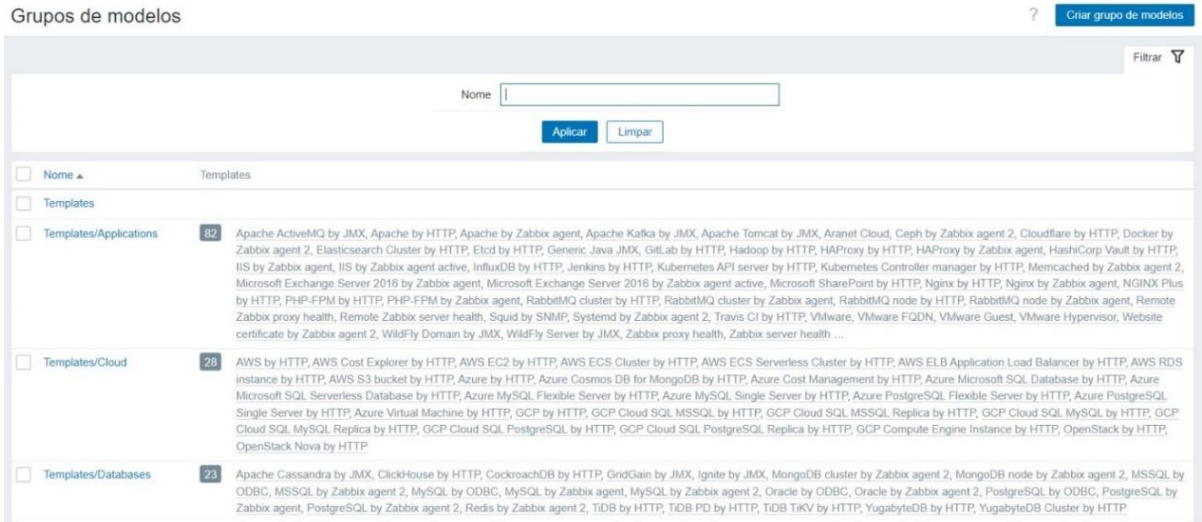
Figura 39: Menu de Alertas



Fonte: Autor

No *Zabbix*, os Grupos de Modelos de *Templates* desempenham um papel fundamental na simplificação e automação do processo de monitoramento de diversos dispositivos. Durante os testes, a funcionalidade foi explorada a partir dos *templates* pré-instalados disponíveis, facilitando a aplicação de configurações padronizadas a múltiplos *hosts* de forma centralizada.

Figura 40: *Templates* do *Zabbix*



Fonte: Autor

Os *templates* são conjuntos de itens de monitoramento, gráficos, *triggers*, e ações predefinidas que podem ser aplicados a diversos *hosts*. Na Figura 40, é possível observar os Grupos de *Templates* organizados no *Zabbix*, os quais permitem que diferentes tipos de dispositivos, como servidores, *switches*, roteadores e estações de trabalho, sejam configurados rapidamente para monitoramento, sem a necessidade de definir manualmente cada parâmetro para cada dispositivo individualmente.

Esse recurso foi particularmente útil para os laboratórios da UFES, uma vez que, ao associar *hosts* aos Grupos de Templates, tornou-se possível implementar rapidamente políticas de monitoramento homogêneas para todos os dispositivos da rede. Isso economiza tempo, reduz a complexidade de configuração e garante consistência nos parâmetros de monitoramento. Com essa abordagem, o *Zabbix* pôde monitorar diversos dispositivos com diferentes funções, aplicando as melhores práticas para cada um deles de forma automatizada.

Os Mapas de Rede no Zabbix são uma funcionalidade poderosa que facilita a visualização gráfica da topologia da rede, permitindo que os administradores de sistemas obtenham uma visão clara e organizada de todos os dispositivos conectados. Durante os testes, foi possível explorar essa funcionalidade e criar mapas de rede detalhados, que representaram visualmente todos os dispositivos monitorados no ambiente de teste.

Na Figura 41, é exibido um exemplo de mapa de rede gerado pela plataforma, destacando a conectividade entre os dispositivos do laboratório e outros elementos da rede. O Zabbix permitiu a criação de mapas personalizados, onde se podia visualizar não apenas os dispositivos, mas também informações em tempo real sobre o status de cada um, como disponibilidade, incidentes e alertas.

Figura 41: Mapas de redes do *Zabbix*

Fonte: Autor

A funcionalidade de Mapas de Rede é extremamente útil para a gestão de configuração de redes, pois facilita a identificação de falhas ou mudanças na topologia. Além disso, a interface gráfica permite o acompanhamento visual da saúde da rede, possibilitando uma resposta rápida e eficaz aos problemas detectados.

A experiência de testar o Zabbix foi bastante enriquecedora e revelou o potencial da ferramenta para o monitoramento e gerenciamento de redes. Desde o início, a instalação e configuração do sistema, incluindo a adição de agentes aos dispositivos, mostrou-se relativamente simples e intuitiva. A funcionalidade de descoberta automática facilitou a inclusão dos dispositivos na rede, e o uso de templates prontos agilizou o processo de configuração, sem a necessidade de ajustes complexos. A partir daí, o sistema apresentou uma interface clara e eficiente para acompanhar o desempenho e a saúde dos dispositivos conectados.

Durante os testes, o Zabbix destacou-se pela abrangência de suas funcionalidades, especialmente em relação ao monitoramento detalhado, à geração de alertas automáticos, à criação de mapas de rede e à gestão de inventários de dispositivos. A possibilidade de configurar notificações de eventos, como a adição de novos hosts, e a integração com relatórios detalhados sobre o estado da rede foram pontos que reforçaram a viabilidade do uso da ferramenta nos laboratórios. Em resumo, o Zabbix

provou ser uma solução robusta e versátil para o gerenciamento de redes, proporcionando controle eficiente e uma visão ampla da infraestrutura de TI.

4.7.3. TESTE FÍSICO: SOLARWINDS

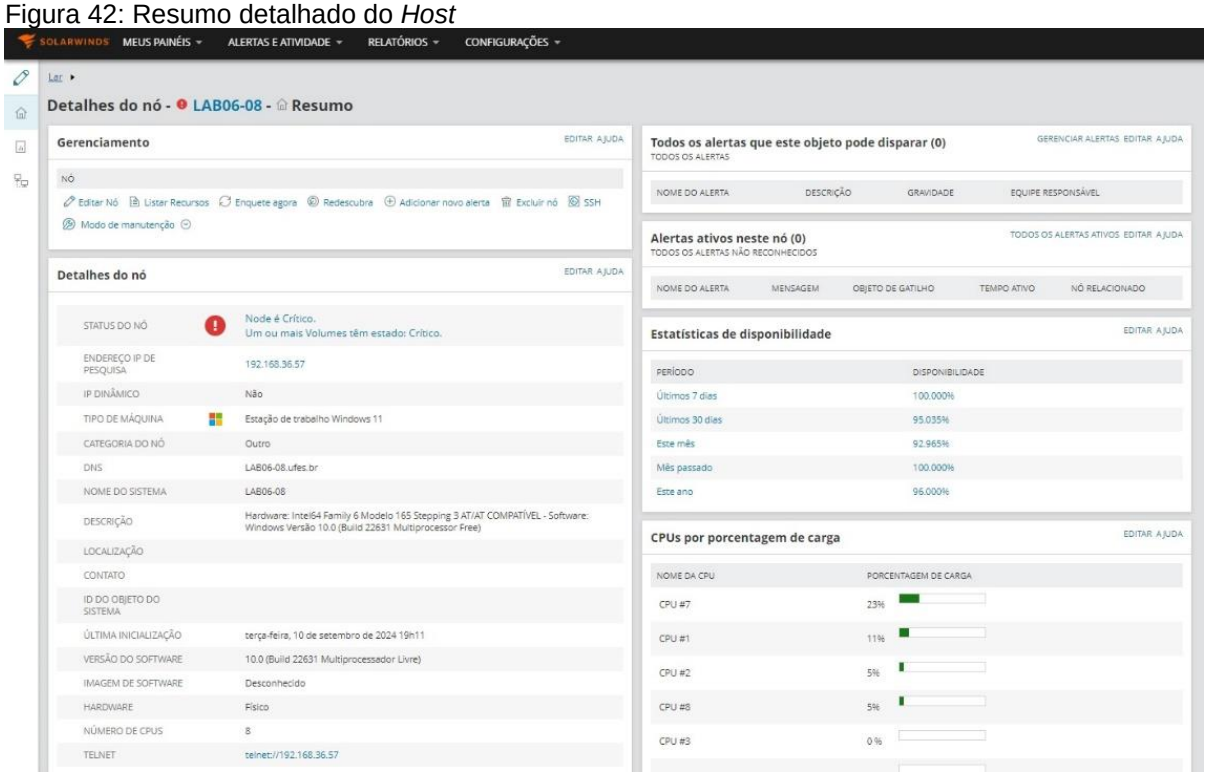
O teste físico do *SOLARWINDS* foi conduzido com o objetivo de verificar, em um ambiente real, a eficácia da ferramenta em comparação ao seu desempenho observado no teste virtual. No ambiente físico, foram exploradas as capacidades de gerenciamento de rede em uma infraestrutura prática, avaliando sua habilidade de descoberta automática de dispositivos, geração de inventários, configuração de backups e emissão de alertas. Diferente do ambiente virtual, onde o desempenho foi limitado à simulação, o teste físico permitiu observar a aplicação direta das funcionalidades no Laboratório de Desenvolvimento de *Software*. Essa análise permitiu identificar possíveis discrepâncias entre os resultados simulados e os obtidos em um cenário real, oferecendo uma visão mais completa do potencial da ferramenta para a gestão de redes no contexto da UFES.

O *SOLARWINDS* armazena as configurações de computadores, *switches* e roteadores por meio de um sistema de gerenciamento centralizado que coleta e mantém registros detalhados de cada dispositivo na rede. Cada dispositivo é identificado e catalogado na interface do *SOLARWINDS*, onde suas configurações são capturadas e armazenadas em um banco de dados. Essa captura é realizada utilizando protocolos como *SNMP*, que permite ao *SOLARWINDS* acessar as configurações de maneira eficiente e em tempo real.

Após a coleta, as configurações são armazenadas de forma estruturada, permitindo que os administradores acessem facilmente os dados quando necessário. O S *SOLARWINDS* também oferece funcionalidades de versionamento, que permitem rastrear alterações feitas nas configurações ao longo do tempo. Isso é crucial para a manutenção da conformidade e para a capacidade de reverter rapidamente a configurações anteriores em caso de falhas ou problemas de desempenho. Além disso, o sistema de *backup* automatizado garante que as configurações sejam regularmente salvas, proporcionando uma camada adicional de segurança e proteção contra perdas acidentais de dados.

Podemos observar com detalhes na Figura 42 como o software *SOLARWINDS* captura as informações dos dispositivos conectados, exemplificando o computador LAB06-08. A ferramenta realiza a coleta de dados em tempo real, identificando e monitorando as principais métricas de desempenho, tais como consumo de *CPU*, uso de memória, estado da interface de rede, entre outros. Esse processo de monitoramento é essencial para a gestão eficiente da rede, pois permite a detecção rápida de anomalias e a geração de alertas automáticos caso algum parâmetro crítico seja excedido. A partir desses dados, o administrador de rede pode agir preventivamente para garantir a estabilidade e o desempenho da infraestrutura.

Figura 42: Resumo detalhado do *Host*

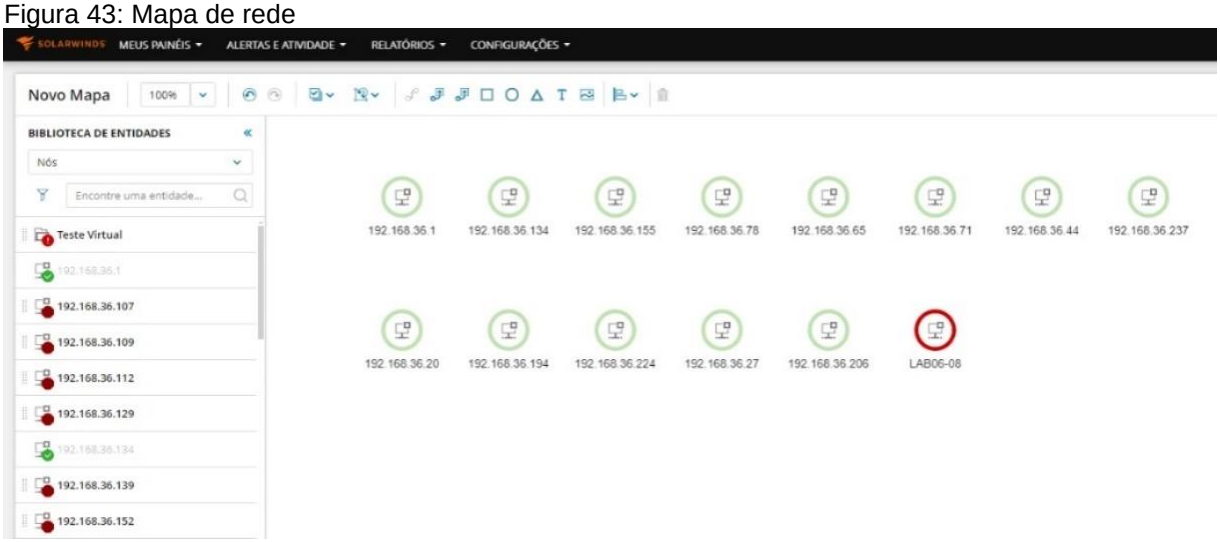


Fonte: Autor

Um ponto que chamou atenção durante o teste foi a facilidade de construir mapas da rede utilizando o *SOLARWINDS*. Essa funcionalidade permite que o administrador visualize, de maneira gráfica e interativa, a topologia completa da rede. O sistema identifica automaticamente os dispositivos conectados e suas inter-relações, exibindo uma representação visual clara dos roteadores, *switches*, servidores, e outros elementos de rede. Esses mapas facilitam a identificação de gargalos e falhas, além de permitir uma navegação intuitiva entre os dispositivos para análise detalhada. Essa visualização gráfica da topologia não só melhora o gerenciamento de configuração, como também simplifica a resolução de problemas e a implementação de alterações

na infraestrutura. Na Figura 43 a seguir, pode-se observar a topologia de rede que a ferramenta *SOLARWINDS* construiu automaticamente.

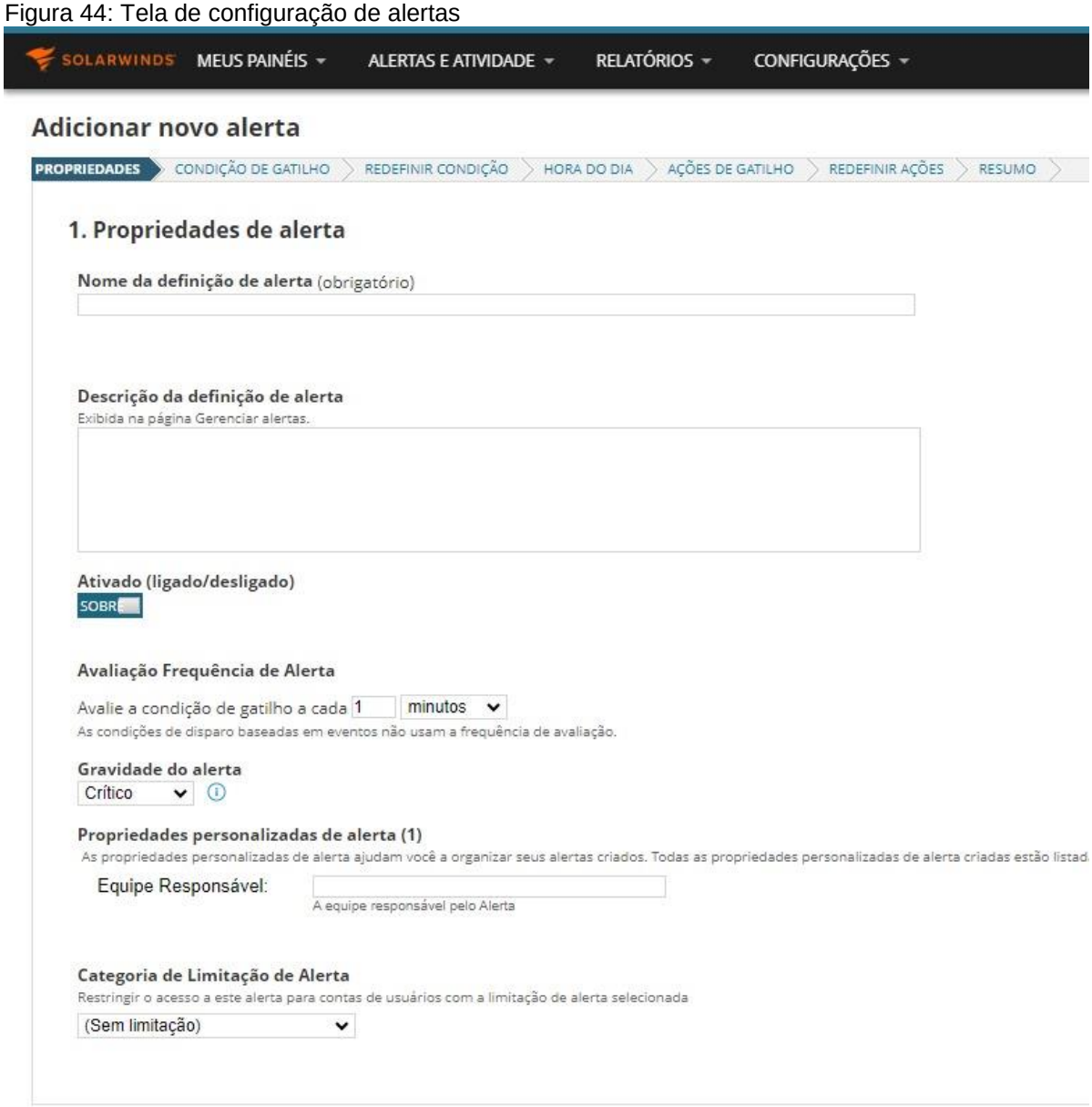
Figura 43: Mapa de rede



Fonte: Autor

Durante o teste físico com o *SOLARWINDS*, foi possível explorar de forma mais aprofundada a funcionalidade de alertas, que desempenhou um papel crucial no monitoramento em tempo real da rede. A ferramenta permitiu configurar notificações automáticas para diferentes cenários, como queda de conexão de dispositivos, falhas em componentes de hardware ou problemas de desempenho. Essas notificações foram personalizadas para serem enviadas por e-mail ou exibidas na interface gráfica da plataforma, como observamos na Figura 44 a primeira tela de configuração de alertas.

Figura 44: Tela de configuração de alertas



Fonte: Autor

A funcionalidade de alertas da ferramenta foi capaz de notificar, de maneira eficiente, problemas relacionados tanto à configuração quanto aos softwares instalados nos dispositivos monitorados, proporcionando uma resposta rápida e assertiva a possíveis falhas na rede.

Um dos *dashboards* que se destacou durante a análise foi a funcionalidade de identificação de todos os endereços *IP* das interfaces de cada dispositivo conectado à rede. Na Figura 45, é possível observar que o computador LAB06-08 possui cinco interfaces distintas, cada uma com seu respectivo endereço *IP* atribuído. Essa visualização detalhada é fundamental para a gestão eficiente da rede, permitindo aos

administradores monitorar o tráfego, identificar possíveis conflitos de *IP* e garantir a correta comunicação entre os dispositivos.

Figura 45: *IPs* de cada interface do LAB06-08

Todos os endereços IP em LAB06-08

EDITAR AJUDA

Search IP Addresses

VERSÃO IP	ENDEREÇO IP
IPv4	**192.168.36.57 (IP de sondagem)**
IPv4	192.168.218.2
IPv4	192.168.56.1
IPv6	fe80::1301:3216:4661:85fc
IPv6	fe80::1355:f513:3870:c76a

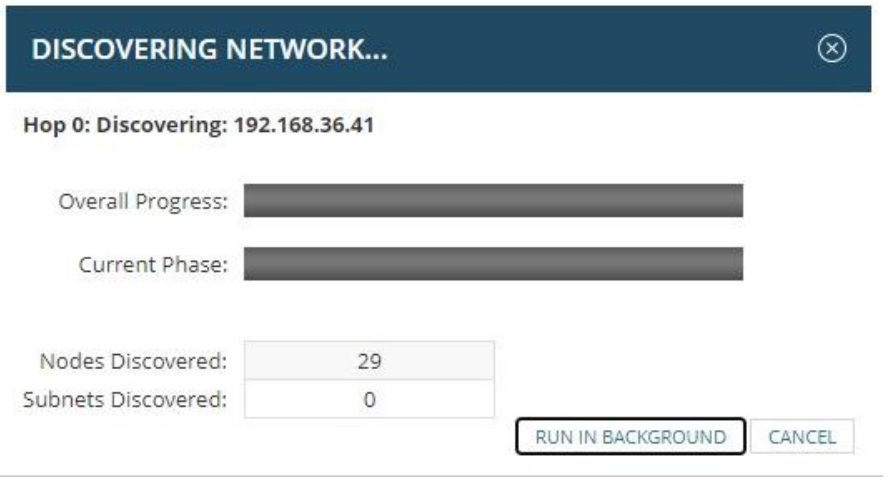
| Mostrar tudo

Fonte: Autor

Além disso, a capacidade de visualizar os endereços *IP* das interfaces em um único painel simplifica o gerenciamento da rede, uma vez que os administradores podem rapidamente diagnosticar problemas de conectividade e realizar manutenções de forma proativa. A apresentação clara dessas informações em um dashboard intuitivo proporciona uma visão abrangente do estado da rede, facilitando a tomada de decisões informadas e a implementação de soluções eficazes para eventuais problemas de configuração ou desempenho.

O processo de configuração da descoberta de rede no *SOLARWINDS* foi um passo crucial para a identificação e monitoramento eficiente dos dispositivos conectados. Inicialmente, foi acessado a interface de configuração de descoberta, onde foi possível definir as regras que orientariam a busca por novos dispositivos na rede. Essas regras incluíram a definição de intervalos de endereços *IP*, tipos de dispositivos a serem incluídos (como servidores, roteadores, *switches*, etc.) e protocolos de descoberta, como *ICMP* (*Ping*) e *SNMP*. Na Figura 46, podemos observar a execução da descoberta de dispositivos do *SOLARWINDS.*

Figura 46: *Descoberta de rede*



Fonte: Autor

Uma vez estabelecidas as regras, foi possível pré-configurar várias opções que facilitariam a integração de novos *hosts* ao ambiente de monitoramento. Por exemplo, foi especificado que fosse feita a adição automática de novos dispositivos à estrutura de gerenciamento assim que fossem descobertos, bem como a atribuição de templates de monitoramento que definiram quais métricas e gráficos seriam aplicados a cada tipo de dispositivo. Além disso, foi viável configurar alertas para notificar automaticamente os administradores quando novos dispositivos eram adicionados à rede ou quando existiam alterações significativas nos dispositivos existentes.

Um ponto negativo significativo que pode representar um desgaste para a Universidade Federal do Espírito Santo é que o *SOLARWINDS* é uma solução paga, com cotações que começam em $ 1.970,00 dólares americanos, o que, na conversão atual, equivaleria a cerca de R$ 10.800,00. Este custo elevado torna a ferramenta inviável para a instituição, especialmente considerando a necessidade de lidar com orçamentos limitados, processos de licitação e outras burocracias associadas à aquisição de sistemas. A gestão de recursos financeiros nas universidades públicas é um desafio constante, e a implementação de uma solução de gerenciamento de configuração de redes que requer um investimento substancial pode comprometer a alocação de verbas para outras áreas críticas. Portanto, a necessidade de uma ferramenta acessível e eficiente é imperativa, o que reforça a escolha da Zabbix como uma alternativa mais apropriada para atender às demandas de monitoramento e gestão de configuração das redes dos laboratórios na UFES.

5. CONCLUSÃO

Os resultados dos testes evidenciaram as diferentes capacidades de cada ferramenta em atender às necessidades de gerenciamento de configuração de redes. O *Zabbix* se destacou entre as demais, quando analisada sob as métricas estabelecidas na metodologia. Comparando com o *SolarWinds*, o *Zabbix* apresentou uma configuração mais intuitiva e acessível, o que facilitou a sua implementação nos ambientes de teste. Enquanto o *SolarWinds*, sendo uma solução paga, exigiria um investimento significativo. O *Zabbix* demonstrou ser uma alternativa viável e econômica para a universidade.

Além disso, o *Zabbix* ofereceu recursos abrangentes de monitoramento que englobavam não apenas dispositivos físicos, mas também serviços e aplicações, proporcionando uma visão holística da infraestrutura de TI. Em comparação, o *SolarWinds*, embora poderoso, apresentava dificuldades em áreas como configuração e usabilidade, resultando em um grau não tão satisfatório. Outro aspecto significativo foi o desempenho superior da *Zabbix* na identificação e gerenciamento de dispositivos conectados à rede, que facilitou a administração e a visibilidade em um ambiente com múltiplos dispositivos e serviços em execução. A capacidade de personalização da ferramenta também permitiu que ela fosse ajustada para atender às especificidades do atual cenário dos Laboratórios de Informática da UFES, tornando-a ainda mais alinhada com as necessidades da instituição. Portanto, pode-se concluir que a Zabbix foi a ferramenta que melhor atendeu aos requisitos propostos neste trabalho, demonstrando ser uma solução robusta e eficiente para o gerenciamento de configuração de redes nos laboratórios de informática da UFES.

Como um trabalho futuro, a implementação do Zabbix pode ser escalonada para abranger toda a rede da UFES em Alegre, não apenas focando na configuração, mas também explorando outras áreas cruciais da gestão de redes, como monitoramento de desempenho, análise de tráfego, gestão de segurança e automação de processos. Essa expansão permitirá uma gestão mais integrada e eficiente da infraestrutura de TI, contribuindo para a otimização dos recursos e melhoria contínua na qualidade dos serviços oferecidos pela universidade.

Além disso, outro trabalho futuro relevante seria o desenvolvimento de uma nova ferramenta com os mesmos propósitos, aproveitando o que há de melhor nos sistemas testados, como o Zabbix, e aprimorando os aspectos que se mostraram menos eficazes. Essa nova solução poderia oferecer uma abordagem ainda mais otimizada para monitoramento e gestão de redes, ajustando-se às necessidades específicas da infraestrutura e superando as limitações identificadas nos sistemas atuais. Dessa forma, a criação de uma ferramenta personalizada pode proporcionar uma visão mais detalhada e precisa das operações de rede, favorecendo ainda mais a tomada de decisões informadas e eficientes.

REFERÊNCIAS

ANDREOLI, Yuri. **Análise Comparativa Entre Ferramentas para Gerenciamento e Monitoramento de Redes.** 2016. 108 f. Monografia (Trabalho de Conclusão de Curso) - Curso Superior de Tecnologia em Análise e Desenvolvimento de Sistemas, Universidade Tecnológica Federal do Paraná, Câmpus Pato Branco. Pato Branco, 2016. Acesso em: 10 de nov. de 2022.

BIESZCAD, A., Pagurek, B., and White, T. ***Mobile agents for network management***. 1998. IEEE Communications Surveys, Acesso em: 29 jan. 2023.

BLACK, Tomas Lovis. **COMPARAÇÃO DE FERRAMENTAS DE GERENCIAMENTO DE REDES.** Instituto de Informática. Universidade Federal do Rio Grande do Sul. 2008. Disponível em: http://hdl.handle.net/10183/15986. Acesso em: 10 de nov. de 2022.

BOUTABA, R.; POLYRAKIS, A. **Projecting FCAPS to Active Networks.** Enterprise Networking, Applications and Services Conference Proceedings. Atlanta: IEEE. 2001. Acesso em: 29 jan. 2023.

CLARA. Ana, Pinto. **SEGREDE: mecanismos para Gerência de Segurança em redes.** 1993. Universidade Federal do Rio Grande do Sul. Disponível em: <http://www.penta2.ufrgs.br/gereseg/kerberos.html>. Acesso em: 28 jan. 2023.

CONER. Douglas E. **Redes de computadores e Internet - 6.ed.** 2016. Bookman. Disponível em: <https://books.google.com.br/books?hl=pt-BR&lr=&id=1nwdDAAAQBAJ&oi=fnd&pg=PR1&dq=o+que+%C3%A9+rede+de+computadores&ots=DslRG2qotd&sig=vWD6qZBI3mgvM9t4FsBEeLkuZy4#v=onepage&q&f=false>. Acesso em: 29 jan. 2023.

ELER, Esdras de O. **Modelo TMN: Aplicação ao Gerenciamento de Redes de Telecomunicações,** 2015. Disponível em: <http://www.teleco.com.br/tutoriais/tutorialmodelotmn>. Acesso em: 28 jan. 2023.

FILHO, Olavo Poleto. **Gerenciamento e Monitoramento de Redes I: Análise de Desempenho.** 2012. Disponível em:

<https://www.teleco.com.br/tutoriais/tutorialgmredes1/default.asp>. Acesso em: 28 jan. 2023.

FOROUZAN, B. A. **Comunicação de dados e Redes de Computadores. 4ª. ed.** São Paulo: McGraw-Hill, 2010. Disponível em: <https://books.google.com.br/books?hl=pt-BR&lr=&id=FIaDr9ZtwXgC&oi=fnd&pg=PR29&dq=Comunica%C3%A7%C3%A3o+de+dados+e+Redes+de+Computadores.+4%C2%AA.+ed&ots=2M4D3A4uRU&sig=Fl5bDRuLVCAlla_EFKIGHO5kiN4#v=onepage&q=Comunica%C3%A7%C3%A3o%20de%20dados%20e%20Redes%20de%20Computadores.%204%C2%AA.%20ed&f=false>. Acesso em: 29 jan. 2023.

FOROUZAN, Behrouz A. **Data Communications and Networking**, 4th ed, New York, McGraw Hill, 2007. Acesso em: 28 jan. 2023.

FOROUZAN, Behrouz A; MOSHARRAF, Firouz. **Redes de Computadores: Uma Abordagem TopDown.** Porto Alegre, AMGH Editora Ltda, 2013**.**

GOROD, A.; SAUSER, B.; BOARDMAN, J. **System-of-systems engineering management: A review of modern history and a path forward.** IEEE Systems Journal, dezembro 2008. Acesso em: 29 jan. 2023.

GOYAL, P.; MIKKILINENI, R.; GANTI, M. **FCAPS in the business services fabric model. 18th IEEE International Workshops on Enabling Technologies: Infrastructures for Collaborative Enterprises.** Groningen: IEEE. 2009. Acesso em: 29 jan. 2023.

ISO 7498-4. **ISO/IEC 7498-4:1989 Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 4: Management framework.** 2006. Disponível em: <https://www.iso.org/standard/14258.html>. Acesso em: 28 jan. 2023.

ISO/IEC/IEEE 24765. **Systems and software engineering – Vocabulary. 1st ed. 2010.** Disponível em: https://www.cse.msu.edu/~cse435/Handouts/Standards/IEEE24765.pdf. Acesso em: 26 de jan. de 2023.

JUNIOR, José Valdemir dos Reis. **Gerência de Redes**. 2012. Universidade Federal do Piauí. Acesso em: 28 jan. 2023.

KOCH. Fernando Luiz. **Agentes autônomos para gerenciamento de redes de computadores**. Universidade Federal de Santa Catarina. 1997. Disponível em: < https://repositorio.ufsc.br/handle/123456789/158121>. Acesso em: 28 jan. 2023.

KUROSE, J. F.; ROSS, K. W. **REDES DE COMPUTADORES E A INTERNET: UMA ABORDAGEM TOPDOWN**. 6ª. ed. São Paulo: Pearson, 2013.

LOPES, Raquel V.; SAUVÉ, Jacques P.; NICOLLETTI, Pedro S. **Melhores Práticas Para Gerência de Redes de Computadores.** 1. ed. Editora Campus, 2002.

MACEDO ET AL. Ricardo Tombesi; Roberto Franciscatto; Guilherme Bernardino da Cunha; Cristiano Bertolini. 2018. **Redes de Computadores. 1.ed.** UAB/NTE/UFSM. Universidade Federal de Santa Maria. Disponível em: <https://repositorio.ufsm.br/handle/1/18351>. Acesso em: 29 jan. 2023.

SATO, Danilo T. **Uso eficaz de métricas em métodos ágeis de desenvolvimento de software.** 2007. Disponível em: https://teses.usp.br/teses/disponiveis/45/45134/tde-06092007-225914/pt-br.php. Acesso em: 26 de jan. de 2023.

SOLARWINDS. **Network Configuration Manager.** 2023. Disponível em: < https://www.solarwinds.com/pt/network-configuration-manager>. Acesso em: 30 jan. 2023.

STALLINGS. William. **SNMP, SNMPv2, SNMPv3 and RMON 1 and 2. 3.ed.** Universidade de Michigan. Disponível em: <https://books.google.com.br/books/about/SNMP_SNMPv2_SNMPv3_and_RMON_1_and_2.html?hl=pt-BR&id=gflSAAAAMAAJ&redir_esc=y>. Acesso em: 29 jan. 2023.

PAESSLER IOT. **Monitoramento de redes e de infraestrutura de TI para ambientes de pequeno e médio porte.** 2023. Disponível em: <https://www.paessler.com/br/prtg/prtg-network-monitor>. Acesso em: 30 jan. 2023.

TERAMOTO, Y. et al. **Managing Networks Independently of the Physical Topology by Service Defined Network.** IEEE 37th Annual Computer Software and Applications Conference Workshops (COMPSACW). 2013. Acesso em: 29 jan. 2023.

VANZ, Giorge. **Comparação de Estratégias para Gerência de Configuração de Redes.** 2016. Universidade Federal de Pernambuco. Disponível em: <https://repositorio.ufpe.br/handle/123456789/22415>. Acesso em: 29 jan. 2023.

VIRTUALBOX. **Welcome to VirtualBox.org!.** 2023. Disponível em: < https://www.virtualbox.org>. Acesso em: 17 nov. 2023.

ZABBIX**. Soluções: Network Monitoring.** 2023. Disponível em: <https://www.zabbix.com/br/network_monitoring>. Acesso em: 29 jan. 2023.