**Bryene Gonçalves Fernandes**

**Monitoramento de redes com protocolo SNMP: um estudo de caso com a ferramenta Zabbix**

**MACAÉ**

**2023**

**Bryene Gonçalves Fernandes**

**Monitoramento de redes com protocolo SNMP: um estudo de caso com a ferramenta Zabbix**

Introdução da monografia apresentada a disciplina Trabalho de Conclusão de Curso I do curso de graduação em Sistemas de Informação, da Faculdade Professor Miguel Ângelo da Silva Santos (FeMASS), para aprovação na disciplina.

Orientador Prof. Esp. Lahir Bockorni

**Macaé**

**2023**

**LISTA DE TABELAS**

[Tabela 1 - Comparativos](#_Toc139316874) 23

[Tabela 2 - Cronograma de Execução](#_Toc139316874) 26

**LISTA DE FIGURAS**

[Figura 1 - O modelo de referência OSI 16](#_Toc139316881)

[Figura 2 -A estrutura de funcionamento dos Gerentes e Agentes através do protocolo SNMP](#_Toc139316882)............18

[Figura 3 - Exemplo de um cenário de rede monitorado pelo Zabbi*x*](#_Toc139316883) 21

SUMÁRIO

[1 INTRODUÇÃO 6](#_Toc79593482)

[2 OBJETIVOS 8](#_Toc79593483)

[3. JUSTIFICATIVA 9](#_Toc79593484)

[4. METODOLOGIA DE PESQUISA 11](#_Toc79593485)

[5. REFERENCIAL TEORICO 13](#_Toc79593486)

5.1 INFRAESTRUTURA DE REDES........................................................................ 14

5.2 GERENCIAMENTO DE REDES..........................................................................14

5.3 MODELO OSI........................................................................................................15

5.3.1 CAMADAS............................................................................................16

5.4 PROCOLO SNMP..................................................................................................18

5.5 ZABBIX.................................................................................................................19

5.5.1 CARACTERÍSTICAS............................................................................20

5.5.2 ARQUITETURA....................................................................................20

5.5.3 COMPARAÇÕES..................................................................................22

5.5.3.1 TABELA DE COMPARAÇÕES...........................................23

[6. ESTRUTURAÇÃO DO TRABALHO .........25](#_Toc79593487)

[7. CRONOGRAMA DE EXECUÇÃO .............26](#_Toc79593488)

[8. REFERÊNCIAS ..............................](#_Toc79593489)27

# 1 INTRODUÇÃO

A gestão eficiente e confiável de redes de computadores é uma prioridade incontestável em um mundo cada vez mais interconectado e dependente da tecnologia. A complexidade crescente das infraestruturas de rede demanda soluções abrangentes que possam monitorar, analisar e solucionar problemas de desempenho e disponibilidade em tempo real.

Nesse contexto, o protocolo SNMP[[1]](#footnote-1) emergiu como uma ferramenta crucial para o monitoramento e gestão de redes, proporcionando um meio padronizado de coletar informações e gerenciar dispositivos de rede de maneira eficiente. Além disso, ambientes de Tecnologias da Informação (TI) modernos, para serem eficientes precisam atender a quatro requisitos básicos: tolerância a falhas, escalabilidade, qualidade de serviço e segurança, porém é praticamente impossível atingir à integralidade. Nesse sentido, o monitoramento pode auxiliar na pronta resposta frente aos problemas e falhas que por ventura venham a ocorrer (Hernantes; Gallardo; Serrano, 2015).

Este projeto tem como foco central a exploração do monitoramento de redes por meio do protocolo SNMP, com um enfoque específico na utilização da ferramenta *Zabbix.* O *Zabbix* é uma plataforma de monitoramento amplamente reconhecida e utilizada, que se destaca por sua capacidade de centralizar informações vitais da rede e apresentá-las de maneira acessível e contextualizada[[2]](#footnote-2). O sistema oferece um conjunto abrangente de recursos que permitem aos administradores de sistemas coletar, processar, analisar e visualizar dados críticos relacionados ao desempenho e à disponibilidade dos recursos de TI.

A proposta de estudo de caso que será apresentada neste projeto visa aprofundar a compreensão sobre a implementação prática do monitoramento de redes utilizando o protocolo SNMP e o *Zabbix.* Serão exploradas as etapas de configuração, coleta de dados, análise de métricas e geração de alertas, examinando como essa abordagem pode contribuir para uma gestão mais eficiente das redes de computadores.

A pesquisa também incluirá a apuração dos benefícios e desafios inerentes ao uso do SNMP e do *software[[3]](#footnote-3)* *Zabbix,* considerando aspectos tais como, escalabilidade, segurança e precisão das informações coletadas. Também serão examinados casos de uso específicos nos quais a combinação dessas tecnologias demonstra seu potencial para otimizar a disponibilidade e o desempenho da rede.

Durante a pesquisa serão utilizados dados reais para aplicar os conceitos e técnicas aprendidas da área de infraestrutura de redes. Ocorrerão experimentos para avaliar a eficácia da ferramenta em potenciais situações de falha, realizando comparações em diferentes abordagens. O interesse pelo tema surge da compreensão de que a utilização desse artefato possa trazer ganhos significativos a diversos profissionais da área.

Nesse contexto, o presente projeto de Trabalho de Conclusão de Curso, visa aprofundar o estudo sobre a análise dos ativos de redes via *software* livre, usando a ferramenta *Zabbix* para monitoramento.

# 2 OBJETIVOS

É objetivo geral do presente projeto:

* Explorar o monitoramento de redes através do protocolo SNMP, com ênfase na utilização da plataforma *Zabbix*, buscando criar uma solução abrangente que permita a coleta eficiente de dados de dispositivos, detecção precoce de problemas, análise, visualização, geração de alertas e automação de tarefas.

**2.1 Objetivos específicos:**

* Realizar uma análise completa da ferramenta *Zabbix*, abordando suas principais características, funcionalidades de monitoramento, arquitetura e capacidades de integração com o SNMP;
* Implementar o monitoramento de ambiente, utilizando o *Zabbix* para coletar informações dos dispositivos de rede via SNMP e criar relatórios para visualização e análise dos dados coletados;
* Realizar testes para avaliar o desempenho do estudo feito, verificando a eficiência da coleta de dados, a latência e a capacidade de escalabilidade;
* Guardar o histórico das informações coletadas para possibilitar análise dos dispositivos e serviços implementados;
* Comparar o uso do protocolo SNMP com a ferramenta *Zabbix* à outras abordagens de monitoramento, destacando as vantagens e desvantagens de cada uma; e
* Identificar como a forma de monitoramento contribuiu para a detecção e resolução de problemas na infraestrutura da rede, analisando o impacto das ações tomadas com base nos dados coletados e possíveis melhorias com oportunidades de soluções futuras.

## 3. JUSTIFICATIVA

Nas últimas décadas, as redes de computadores têm assumido um papel de importância inquestionável em praticamente todos os setores, seja no âmbito de órgãos públicos ou empresas privadas. A sua presença é tão fundamental que a estabilidade e o desempenho da infraestrutura de rede tornaram-se requisitos críticos. Isso se deve ao fato de que as redes de computadores atuam como o alicerce das operações, fornecendo suporte indispensável para a execução das aplicações que alimentam os processos organizacionais. Atualmente, as redes estão presentes não apenas nas mais diversas organizações, mas também em nossos lares, visto que é cada vez mais presente o compartilhamento de informações, além do hábito de assistir filmes, ouvir músicas, jogar e conversar com amigos através de chamadas telefônicas e vídeo telefônicas (Tanenbaum, 2003).

Diante desse contexto, é imperativo compreender a relevância de uma análise mais profunda da infraestrutura da rede e, em particular, do serviço de monitoramento de rede. Quando consideramos a rede como o pilar da infraestrutura de Tecnologia da Informação (TI), fica evidente que sua falha pode ter consequências críticas. A interrupção do fluxo de informações, vital para o funcionamento de aplicativos e operações de negócios, pode resultar em prejuízos financeiros significativos, além de comprometer a reputação e a credibilidade de qualquer organização.

Ademais, este trabalho se propõe a explorar em detalhes a importância do monitoramento de redes de computadores, com foco na implementação do Protocolo SNMP e o uso da ferramenta *Zabbix* como estudo de caso. Ao analisar como o monitoramento eficaz pode fornecer uma resposta rápida e precisa ao estado da infraestrutura computacional, esperamos destacar sua relevância como um serviço estratégico em um ambiente onde a informação é base da operação. Além disso, será apurada à busca para identificar como a implementação adequada do monitoramento pode contribuir para a otimização do desempenho da rede, a segurança dos dados e, em última análise, para o sucesso contínuo das organizações no ambiente cada vez mais interconectado e dependente da tecnologia.

O objeto de pesquisa deste projeto será a concentração em entender como protocolo SNMP é utilizado para coletar informações e gerenciar dispositivos de rede, e como o *software Zabbix* é empregado para implementar um sistema de monitoramento eficiente e confiável em um ambiente real, podendo contribuir para a melhoria da disponibilidade, desempenho e segurança das redes de computadores.

Espera-se, com esta proposta de pesquisa, contribuir para a compreensão dos principais conceitos e técnicas utilizadas no gerenciamento de redes, bem como para o desenvolvimento de soluções mais eficientes e precisas nessa área.

Dessa forma, o problema de pesquisa que se formula é, quais são as melhorias proporcionadas pelo uso da plataforma *Zabbix* no contexto do protocolo SNMP, principalmente no que diz respeito à coleta de dados, reforço da segurança da rede e configuração eficaz de alertas para identificação e solução de problemas de rede, e quais são os resultados alcançados por meio dessa abordagem?

Os resultados esperados da análise incluem a identificação das melhorias concretas trazidas pelo *Zabbix* em relação ao protocolo SNMP, com foco nas áreas mencionadas. Isso pode incluir a demonstração de um processo de coleta de dados mais eficiente, exemplos de aprimoramentos na segurança da rede e casos de sucesso na configuração de alertas precisos e oportunos para problemas em redes de computadores.

Ao explorar esses aspectos, a pesquisa visa contribuir para o entendimento do valor agregado pela adoção do *Zabbix* em um ambiente de monitoramento baseado em SNMP, fornecendo informações relevantes para profissionais de redes, administradores de sistemas e interessados em otimizar a gestão de infraestruturas de rede por meio dessa abordagem integrada.

Por fim, este trabalho busca contribuir para o conhecimento e a compreensão das práticas de monitoramento de redes, oferecendo uma compreensão valiosa para profissionais de redes, administradores de sistemas e outros interessados na otimização da infraestrutura de TI. Através desse estudo, espera-se destacar a importância do protocolo SNMP e da ferramenta *Zabbix* como recursos essenciais para a gestão eficaz das redes modernas, proporcionando uma base sólida para a tomada de decisões informadas e proativas.

## 

## 4. METODOLOGIA DE PESQUISA

A metodologia deste estudo consistirá em um estudo de caso experimental. Relacionado aos objetivos é um estudo de caso explicativo, pois busca causas e explicações para os dados observados, em outras palavras, os fatores determinantes desses dados. Associado aos procedimentos técnicos, é uma pesquisa experimental, pois é feita a manipulação de variáveis ou parâmetros do ambiente de rede, permitindo a medição e análise de resultados consequentes, ocasionando um estudo de caso.

Ao coletar os dados através do experimento, pretende-se analisar os resultados obtidos de forma que seja possível identificar se existe um padrão de falhas ao uso ou desuso da ferramenta, e quais as vantagens apresentadas ao inseri-la. Posteriormente, serão realizadas leituras críticas e análises sistemáticas dos artigos selecionados, com o objetivo de identificar as principais abordagens e soluções utilizadas para aprimoramentos na segurança da rede, bem como suas vantagens e limitações. Essa análise crítica será realizada com o auxílio de ferramentas de análise de dados, como *software* de coleta de informações e gerenciamento de dispositivos de rede.

Baseado nas análises obtidas, a pesquisa terá como foco o estudo de caso, em que será aplicado um ambiente virtual simulado, contendo as problemáticas identificadas nos levantamentos, baseado em recursos *Open Source[[4]](#footnote-4)* será utilizado para analisar a eficiência do *Zabbix* ao ser utilizado junto ao protocolo SNMP. O sistema será implementado e configurado de acordo, com especial ênfase na definição de parâmetros de monitoramento e na seleção dos indicadores a serem coletados por meio do protocolo. Esse estudo de caso permitirá avaliar a eficácia do *software* em um cenário específico, além de possibilitar a identificação de problemas reais e oportunidades de solução na aplicação. Pois problemas reais persistem, visto que as preocupações relacionadas à perda de dados se intensificam com o avanço da tecnologia.

Além disso, serão criados relatórios personalizados para facilitar a visualização e análise dos dados monitorados, que estarão em um sistema de armazenamento de dados, garantindo uma análise aprofundada. Isso será realizado considerando as opções de armazenamento oferecidas pelo *Zabbix* ou alternativas compatíveis, garantindo a integridade e acessibilidade dos dados históricos e para avaliar a eficácia do sistema de monitoramento desenvolvido, serão realizados testes de desempenho.

A capacidade de escalabilidade do *Zabbix* será testada, aumentando gradualmente a carga de dispositivos monitorados e monitorando o desempenho em cada fase. O estudo também incluirá uma comparação detalhada entre o uso das ferramentas em conjunto e outras abordagens de monitoramento, com o objetivo de destacar as vantagens e desvantagens de cada método, incluindo eficiência, escalabilidade, facilidade de implementação e custos associados.

Ademais, os resultados da análise serão utilizados para elaborar uma discussão crítica e aprofundada sobre as aplicações de *softwares* de monitoramento e gestão de redes, proporcionando um meio padronizado de coletar informações e gerenciamento de dispositivos de rede de maneira eficiente, abordando seus pontos fortes e limitações.

Para promover o aprofundamento no estudo, serão examinados diversos elementos que, quando combinados, representarão o sistema de infraestrutura de rede real. Isso inclui a avaliação de ferramentas de análise de dados, a configuração do ambiente *Zabbix Server*, a utilização da ferramenta de emulação *VirtualBox* e o emprego do *Cisco Packet Tracer* para a simulação de redes de computadores. Será dada especial atenção a diferentes tipos de conexões, com interfaces conectadas a dispositivos, possibilitando a interconexão de redes com o propósito de conferir ao servidor *Zabbix* uma interface de diagnóstico.

Por meio desta pesquisa será possível efetuar análises quantitativas, qualitativas e quanti-qualitativas, dos benefícios da implantação do sistema. A avaliação dos resultados obtidos pela análise de dados quantitativa será realizada por meio de análise do tráfego de dados, tempo de resposta e outras métricas relevantes como a utilização de CPU, memória, espaço em disco, status de serviços, comparação de protocolos e entre outros, para o problema em questão.

Através da análise qualitativa, será possível quantificar a redução no tempo de resposta para resolução de problemas e o tempo de inatividade dos equipamentos, serviços e sistemas. Por outro lado, a abordagem quali-quantitativa se manifestará na análise dos dados históricos, combinando a avaliação quantitativa das variações com a análise qualitativa, revelando eventos ou problemas específicos que podem não ser imediatamente perceptíveis somente por meio de dados numéricos.

Por fim, serão elaboradas conclusões a partir dos resultados da análise crítica e da análise de dados, a fim de responder aos objetivos propostos na pesquisa, bem como discutir possíveis limitações e oportunidades de futuras pesquisas na área monitoramento de informações de rede.

### 

### 5. REFERENCIAL TEORICO

A administração eficaz das redes de computadores é essencial para garantir o funcionamento contínuo de sistemas de informação e a infraestrutura tecnológica em um mundo cada vez mais dependente da conectividade. Nesse contexto, o monitoramento de redes desempenha um papel fundamental, permitindo a supervisão constante do desempenho, segurança e disponibilidade dos dispositivos e serviços em uma rede. O protocolo SNMP emergiu como um padrão universal para a gestão de dispositivos de rede, possibilitando a coleta de informações vitais a partir de uma variedade de equipamentos, como roteadores, switches e servidores.

Este protocolo, em conjunto com ferramentas de monitoramento, como o *Zabbix*, oferece aos administradores de rede a capacidade de acompanhar o estado dos ativos de rede e responder proativamente a eventos críticos. Neste referencial teórico, será explorado os conceitos fundamentais relacionados às redes de computadores, monitoramento de redes, o protocolo SNMP e a ferramenta *Zabbix*, estabelecendo a base para a compreensão do estudo de caso que irá investigar a implementação dessas tecnologias em um ambiente simulado de gerenciamento.

**5.1 Infraestrutura de Redes**

Conforme enfatizado por Miranda (2008), o conceito de uma "rede de computadores" abrange a interconexão de computadores e todos os dispositivos eletrônicos essenciais para estabelecer e manter essa conexão. Essa interligação tem como propósito assegurar a continuidade da comunicação e a capacidade de compartilhamento de dados, seja em âmbito local ou remoto.

A utilização mais comum das redes de computadores é conectar computadores pessoais, estações de trabalho e infraestruturas empresariais, com o propósito de viabilizar a troca de informações e o compartilhamento de recursos. Redes locais (LANs), por sua vez, se destacam em relação a outros tipos de redes por três características distintas: elas operam em um escopo geograficamente limitado, normalmente empregam meios de transmissão baseados em cabos para conectar as máquinas, e podem ser implementadas em uma variedade de topologias, como destacado por Tanenbaum (2003).

Pode-se destacar algumas topologias físicas:

* **Estrela:** A rede se configura com a figura de um nó central ligado a todos os outros nós e por onde é passado todas as mensagens (Soares & G Colcher, 1995);
* **Anel:** Os dispositivos são conectados em série, formando um circuito fechado. Eles trabalham como repetidores, até que a mensagem seja retirada da rede pelo nó de destino (Soares & G Colcher, 1995);
* **Barramento:** Todos os nós se ligam ao mesmo meio de transmissão e cada nó pode ver todas as informações transmitidas (Soares & G Colcher, 1995);
* **Malha**: Consiste na comunicação total entre os equipamentos, ou seja, em uma rede com cinco elementos, cada um deles possuirá quatro conexões distintas. Quando um novo nó é inserido este terá que ser ligado a todos os outros.
* **Árvore:** Existe uma estrela central onde outros ramos menores se conectam. A ligação entre nós é realizada através de derivadores e as conexões das estações realizadas da mesma maneira que no sistema estrela padrão. Cada ramificação significa que o sinal deverá se propagar por dois caminhos diferentes (Fernández, 2019);
* **Ponto-a-ponto:** o computador central é conectado a um equipamento de comunicação de entrada e saída por uma única linha (Fernández, 2019);

A escolha da topologia certa em uma rede é de fundamental importância, pois essa decisão afeta diretamente a eficiência, a escalabilidade, a confiabilidade e a manutenção do sistema. Cada topologia possui características únicas que atendem a diferentes necessidades e cenários. A seleção adequada da topologia permite otimizar o desempenho da rede, minimizar problemas de congestão, garantir a disponibilidade dos serviços e simplificar a administração, contribuindo assim para o sucesso e a eficácia das operações da organização. Portanto, a decisão sobre a topologia deve ser cuidadosamente ponderada, levando em consideração os requisitos específicos da rede e as metas a serem alcançadas.

**5.2 Gerenciamento de Rede**

O gerenciamento de redes envolve uma variedade de tarefas, como monitorar o desempenho da rede, identificar e resolver problemas, configurar dispositivos de rede, garantir a segurança dos dados e garantir a disponibilidade contínua dos recursos de rede. Para tanto, são empregadas técnicas e protocolos específicos, bem como ferramentas de *software*, a fim de manter a integridade e o funcionamento ininterrupto das redes, atendendo às necessidades das organizações e dos usuários finais. Esse campo de estudo e prática é fundamental para a infraestrutura digital moderna, e seu aprimoramento contínuo desempenha um papel vital na garantia da conectividade global e na entrega de serviços de alta qualidade.

Com base em levantamento, Lessa (1999) apresenta que enquanto 30% dos custos de uma infraestrutura computacional estão diretamente associados à aquisição de *hardware[[5]](#footnote-5)*, os 70% restante dizem respeito à manutenção e suporte aos recursos e serviços nela contida. Desta forma, o monitoramento da infraestrutura computacional desempenha um papel fundamental na manutenção da operação ininterrupta dos serviços oferecidos. Essa prática é essencial para assegurar que a qualidade dos serviços seja mantida em níveis satisfatórios ao longo do tempo, contribuindo de forma decisiva para a confiabilidade e eficiência do ambiente de rede.

**5.3 Modelo OSI**

O modelo OSI[[6]](#footnote-6), desenvolvido pela ISO[[7]](#footnote-7), é um *framework*[[8]](#footnote-8) que visa padronizar a comunicação de rede em sete camadas distintas. Estas camadas foram concebidas com base em princípios específicos para garantir a interoperabilidade e a eficiência das redes de computadores. Cada camada desempenha um papel importante na comunicação de dados e segue os seguintes princípios:

* Cada camada deve ser o mais independente possível das demais, o que significa que as mudanças em uma camada não devem afetar as demais;
* Cada camada possui funções bem definidas e específicas (Tanenbaum, 2003);
* A comunicação de dados é encapsulada em cada camada, o que significa que os dados são empacotados com informações adicionais em cada camada à medida que são transmitidos pela rede. Isso ajuda a garantir a integridade dos dados e a adição de funcionalidades específicas em cada camada;
* Os detalhes internos de uma camada não são visíveis para as camadas superiores;
* O modelo OSI é projetado para ser independente de tecnologia;
* O número de camadas deve ser grande o bastante para que funções distintas não precisem ser desnecessariamente colocadas na mesma camada e, pequeno o suficiente para que a arquitetura não se torne difícil de controlar (Tanenbaum, 2003).

De acordo com a figura, pode-se visualizar o modelo de referência OSI, composto por sete camadas.

Figura 1 - O modelo de referência OSI

****

*Fonte: (Tanenbaum, 2003, p. 26).*

Esse modelo é um padrão utilizado para entender e descrever a estrutura das redes de computadores, serve como um guia para o desenvolvimento de protocolos de rede e é uma ferramenta fundamental para o entendimento das operações de redes de computadores, na qual cada camada desempenha um papel específico na comunicação de dados.

**5.3.1 Camadas**

Cada camada desempenha funções específicas e se comunica com as camadas adjacentes por meio de protocolos padronizados, permitindo a interoperabilidade de dispositivos em uma rede.

* **Camada 1 - Física:** é responsável pela estruturação de *hardware*, ou seja, a transmissão de bits por um canal de comunicação;
* **Camada 2 - Enlace:** é responsável pela troca de dados entre um sistema final e a rede a qual está conectado;
* **Camada 3 - Rede:** Conhecida como IP, esta camada tem como função o roteamento entre as várias redes;
* **Camada 4 – Transporte:** Conhecida como TCP[[9]](#footnote-9),garante que todos os dados chegam no destino na mesma ordem em que foram enviados. Aceita dados da camada acima dela e os divide em unidades menores, repassa essas unidades à camada de rede e garante que todos os fragmentos chegarão corretamente à outra extremidade (Tanenbaum, 2003);
* **Camada 5 – Sessão:** Permite estabelecer sessões de comunicação entre os usuários de diferentes máquinas;
* **Camada 6 – Apresentação:** Está relacionada a sintaxe e à semântica das informações transmitidas, e
* **Camada 7 – Aplicação:** Responsável pela utilização das mensagens, possui vários protocolos necessários para o usuário. O protocolo mais usado é o HTTP[[10]](#footnote-10) quando digitado um endereço no navegador; ao utilizar esse protocolo, envia o nome da página desejada ao servidor que hospeda a página, o servidor então transmite a página ao navegador.

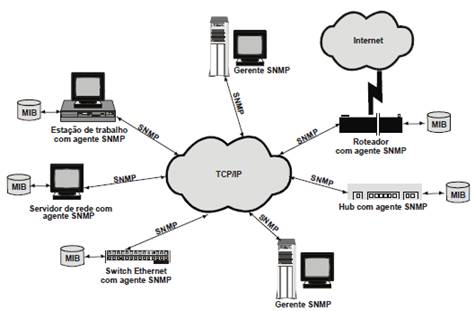
**5.4 Protocolo SNMP**

Um dos principais papéis desempenhados por um administrador de rede é a coleta precisa de informações relacionadas aos serviços e à infraestrutura que compõem sua rede. Existem diversas ferramentas e soluções disponíveis para simplificar a obtenção e processamento desses dados, e muitas delas se baseiam na tecnologia conhecida como SNMP. Está implementado na sétima camada do modelo OSI (Camada de Aplicação) e possui gerência típica de redes TCP/IP. Este protocolo foi criado para fornecer fácil inserção e baixo custo para ser implantado nos diversos dispositivos de gerenciamento de redes como roteadores, switches, servidores e outros dispositivos de rede.

Existem algumas versões do protocolo SNMP, a primeira foi adotada como padrão em 1989 e possuía falhas no quesito de segurança. O SNMPv2 (segunda versão) fornece gerenciamento de rede centralizado e distribuído incluindo aprimoramentos na sua estrutura e gerenciamento. O SNMPv3 (terceira versão), foi criado para solucionar as questões de segurança da primeira e segunda versão, fornecendo acesso seguro às informações de gerenciamento por meio de autenticação e criptografia de pacotes.

A arquitetura de gerência utilizando o SNMP conta com quatro elementos básicos: os nós gerenciados (agentes), as estações de gerenciamento (gerentes), as informações de gerenciamento (MIBs) e o protocolo de gerenciamento (SNMP), conforme a Figura 2.

Figura 2 - A estrutura de funcionamento dos Gerentes e Agentes através do protocolo SNMP.



*Fonte: (Teleco, s.d.).*

A MIB[[11]](#footnote-11) é um banco de dados lógico que armazena informações estatísticas de configuração e de status, relativas a todos os possíveis objetos gerenciáveis da rede. As MIB’s descrevem a estrutura de gestão dos dados de um subsistema de um dispositivo por meio do uso de denominações hierárquicas contendo os OID’s[[12]](#footnote-12).

Quando é necessário obter informações de um dispositivo de rede usando o SNMP, é utilizado o protocolo para consultar objetos específicos na MIB, referenciando o OID do objeto em questão. Identificadores de objetos são identificáveis por *strings* [[13]](#footnote-13)de números separados por pontos. Existem dois tipos de objetos gerenciados:

* Escalar: Objetos definidos por uma única instância de objeto (ou seja, só pode haver um resultado).
* Tabular:Objetos definidos por diversas instâncias de objetos relacionados agrupadas em tabelas MIB.

Os MIB’s organizam as OID’s de forma hierárquica, possibilitando sua representação em uma estrutura de árvore. Essa árvore abrange todos os recursos gerenciáveis de diversos produtos, organizados de maneira sistemática. Cada ramo dessa árvore é identificado por um número e um nome exclusivo, atribuído com base no caminho completo que conduz do topo da árvore até o ponto específico.

**5.5 Zabbix**

*Zabbix* é um *software* *Open Source* capaz de monitorar a disponibilidade e o desempenho da infraestrutura de diversos parâmetros de uma rede (Horst; Pires; Déo, 2015), sendo ideal para monitorar e controlar o funcionamento dos ativos e seus serviços. Possui um sistema de notificações altamente personalizável, que oferece aos usuários a flexibilidade de configurar alertas por e-mail, mensagens instantâneas e SMS sempre que ocorre um evento em um dos ativos gerenciados. Além disso, quando configurado adequadamente, o sistema permite a execução remota de comandos, simplificando a resolução de problemas nos dispositivos monitorados.

O sistema possui agentes de alto desempenho integrados, com suporte para uma variedade de sistemas operacionais, incluindo GNU/Linux, Microsoft® Windows®, IBM® AIX® e entre outros. Ademais, oferece opções de monitoramento tanto com agentes SNMP ou IPMI, garantindo versatilidade na coleta de dados. A autenticação de usuário é altamente segura, com criptografia dos dados e permissões flexíveis.

O *software* oferece interface web própria, suporte à diversos sistemas, agentes nativos para maioria dos sistemas operacionais, capacidade de monitorar diretamente o protocolo SNMP (v1,v2,v3), integração com banco de dados, geração de gráficos, envio de alertas e customização.

**5.5.1 Características**

O sistema de gerenciamento de redes desempenha funções cruciais em várias áreas. Com base nessas funções, o *Zabbix* apresenta as seguintes características distintivas:

* Prove ao administrador de sistemas informações em tempo real sobre o desempenho de um servidor;
* Prevê comportamentos futuros de parâmetros monitorados usando um algoritmo de mínimo quadrado;
* Monitoramento do SLA[[14]](#footnote-14);
* Usado para o monitoramento de arquivos de logs;
* Capaz de verificar a integridade do servidor, e
* Permite análise de disponibilidade.

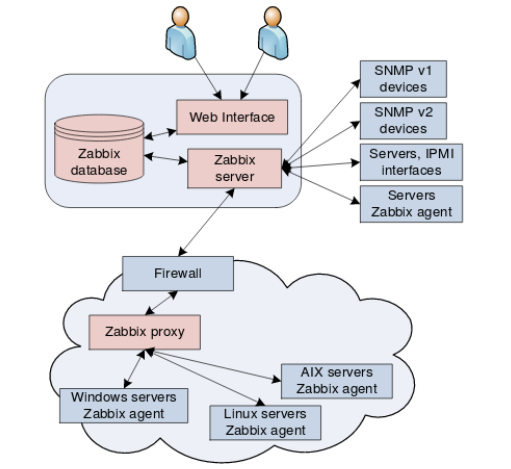
**5.5.2 Arquitetura**

A arquitetura básica do *Zabbix*, geralmente é feita em um único servidor, mas pode haver razões para separar seus elementos. Uma instalação básica do *Zabbix* contém ao menos o servidor *Zabbix*, a interface web e o banco de dados. No entanto, há outros componentes, como o agente e o proxy, que também fazem parte de sua arquitetura.

Conforme ilustrado na figura abaixo, o sistema se compõe de diversos elementos-chave,

criando uma estrutura modular que permite um monitoramento escalável e versátil de recursos de rede e sistemas.

Figura 3 - Exemplo de um cenário de rede monitorado pelo Zabbix.



*Fonte: (Horst, Pires e Déo, 2015, p. 86).*

Na Figura 3, podemos examinar os diversos componentes da arquitetura do *Zabbix,* cada um desempenhando um papel crucial no sistema de monitoramento. Esses componentes têm finalidades específicas:

* Servidor *Zabbix*: Este é o núcleo do sistema, onde todas as informações enviadas pelos agentes dos dispositivos monitorados são centralizadas. Ele coordena a coleta de dados, processa eventos e notificações e fornece a base para a análise e tomada de decisões.
* Banco de dados *Zabbix*: O banco de dados é o repositório das informações de monitoramento coletadas a partir dos dispositivos. Tanto o Servidor *Zabbix* quanto a Interface Web acessam e consultam o banco de dados para obter dados históricos e informações atuais.
* Interface Web *Zabbix*: Esta é uma aplicação web que oferece uma maneira conveniente de acessar e visualizar as informações provenientes dos agentes. Ela fornece painéis de controle, relatórios e gráficos, permitindo aos administradores e equipes de operação monitorar o estado da rede e dos sistemas de forma eficaz.
* Agente *Zabbix*: O Agente *Zabbix* é o componente que reside nos dispositivos gerenciados. Ele é responsável por coletar dados locais, como uso de CPU, memória e outros recursos, e enviá-los de forma proativa para o Servidor *Zabbix*. Isso possibilita a monitorização em tempo real do desempenho e da saúde dos dispositivos.
* Proxy *Zabbix*: O Proxy *Zabbix* é uma parte opcional do sistema que desempenha um papel fundamental na escalabilidade. Ele permite a distribuição da coleta de dados de gerenciamento, aliviando a carga do Servidor *Zabbix* principal e, assim, possibilitando um monitoramento eficiente e escalável em redes complexas ou de grande porte.

Esses componentes trabalham em conjunto para fornecer uma solução completa de monitoramento de rede e sistemas, oferecendo aos administradores as ferramentas necessárias para garantir o desempenho e a confiabilidade de suas infraestruturas.

**5.5.3 Comparações**

O *Zabbix* é uma poderosa ferramenta de monitoramento de código aberto, projetada para rastrear o desempenho e a disponibilidade da infraestrutura de TI. Assim como já mencionado nos capítulos anteriores. Porém, é importante destacar que, embora seja uma ferramenta notável, não é o único *software* no mercado com essas funcionalidades. Entre as alternativas disponíveis, encontra-se o *Nagios Core,* que também oferece recursos sólidos de monitoramento e alerta. A escolha entre o *Zabbix* e o *Nagios Core* dependerá das necessidades específicas da sua organização, bem como das preferências individuais. Ambas as ferramentas têm seus méritos e podem ser personalizadas de acordo com os requisitos do seu ambiente de TI.

Assim como na outra ferramenta, é possível instalar um agente do *Nagios* na máquina-alvo. Dessa forma, a comunicação ocorre entre o servidor e o agente, com este último instalado na máquina a ser monitorada, aguardando solicitações feitas pelo servidor. Quando uma solicitação é recebida, como a quantidade de espaço livre em um disco específico, o agente fornece as informações solicitadas e as envia de volta ao servidor. Além disso, a coleta de dados também pode ser realizada utilizando o protocolo SNMP.

Ambas as ferramentas oferecem um equilíbrio ideal entre simplicidade e profundidade. Em termos gerais, tanto o *Zabbix* quanto o *Nagios Core* proporcionam uma visão abrangente da rede conectada. A qualidade de ambos os produtos torna desafiante a escolha do melhor entre eles, mas é possível analisar diversos pontos importantes em cada um por meio da avaliação de recursos como dashboards, configurabilidade, alertas, suporte a protocolos, autodescoberta e plugins. O objetivo é expor de forma eficaz o que cada produto tem a oferecer e determinar qual deles proporciona a melhor experiência de monitoramento.

**5.5.3.1 Tabela de Comparações**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **ZABBIX** | **NAGIOS CORE** | **VENCEDOR** |
| **Dashboard e**  **Interface de usuário** | Dashboard de alta qualidade e pode ser customizada, oferecendo uma experiência mais clara. | Dashboard de alta qualidade, disponibiliza informação básica, como o status de dispositivos, mas não oferece o mesmo nível de qualidade e clareza de display como Zabbix. | ZABBIX |
| **Configuração** | É outra característica no qual a Zabbix se sobressaí, já que permite que você altere as configurações através de uma interface na web. | Força o usuário a inserir as configurações como arquivos de texto. | ZABBIX |
| **Visualização** | Tem seus gráficos premium disponíveis diretos da caixa. | Não oferece os gráficos por default, entretanto, se fizer download através do plugin NagVis é possível monitorar a rede através do uso de gráficos. | ZABBIX |
| **Interface Web** | Ele apresenta uma interface web dedicada que é altamente conveniente para implementações e oferece a capacidade de configurar seu ambiente de monitoramento por meio de uma interface de usuário moderna e amigável. | Ele possui uma interface web exclusiva que é conveniente para implantações. Porém, apresenta limitações na interação com o Nagios Core. Por exemplo, é possível realizar tarefas básicas, como verificar o estado da rede e gerar relatórios. Mas capacidades é limitada. Além disso, é importante mencionar que a interface sofre de uma aparência desatualizada. | ZABBIX |
| **Autodescoberta** | Inclui uma ferramenta de autodescoberta que pode buscar por dispositivos através de um alcance de IP. | Inclui uma ferramenta de autodescoberta, com o plugin NagiosQL, pode acionar autodescoberta para achar dispositivos conectados; essa é uma das poucas áreas no qual o Nagios Core tem uma vantagem visível sob a Zabbix. | ZABBIX |
| **Suporte de Protocolo** | Oferece suporte para HTTP, FTP, SMTP, SNMP, POP3, SSH e MySQL. | Oferece suporte para HTTP, FTP, SMTP, SNMP, POP3, SSH e MySQL. | EQUIVALENTES |
| **Alertas e Notificações** | Pode optar por receber alertas através de e-mail e SMS, e também pode customizar mensagens e determinar uma corrente de escala. | Alertas e notificações são oferecidas direto da caixa; você pode optar por receber alertas através de e-mail e SMS e o Nagios Core oferece vários níveis de alerta, mas não tem a customização oferecida pela Zabbix. | ZABBIX |
| **Templates de Monitoramento** | Oferece para FTP, HTTP, HTTPS, IMAP, LDAP, MySQL, NNTP, SMTP, SSH, POP e Telnet. | Não possui. | ZABBIX |
| **Plugins** | Não possui | Oferece possibilidades extensivas de plugins adicionais. | NAGIOS CORE |
| **Comunidade** | 80,000 integrantes. | 67,000 integrantes. | ZABBIX |
| **Preço** | Gratuito. | Freemium | EQUIVALENTES |

Tabela 1 - Comparativos

Após avaliação minuciosa, fica claro que ambas as ferramentas possuem seus pontos fortes e se adequam a diversas necessidades e preferências. A seleção entre o *Zabbix* e o *Nagios Core* estará intrinsecamente ligada às particularidades da infraestrutura de TI, às funcionalidades desejadas e ao nível de familiaridade da equipe de operações com cada uma dessas plataformas.

# 

# 6. ESTRUTURAÇÃO DO TRABALHO

O trabalho de conclusão de curso apresentado terá sua estrutura em quatro capítulos. O primeiro capítulo é formado pela introdução do assunto, objetivo geral, e também os objetivos específicos da pesquisa, seguida pela justificativa que expõe a importância do tema metodologia aplicada para fazer a pesquisa.

**No segundo capítulo, será apresentada uma explicação detalhada dos conceitos relacionados à infraestrutura de redes e dos benefícios associados ao monitoramento eficaz. Demais, serão abordados os princípios do gerenciamento de redes, sua relação com os usuários e a relevância do modelo OSI para o estudo de caso. Para além d**a introdução aos protocolos de forma geral e após, será feito o aprofundamento ao protocolo SNMP e sua estrutura. Por conclusão, será exposta uma breve explicação sobre formas de monitoramento eficazes desses protocolos.

O terceiro capítulo contará com explicações embasadas sobre a ferramenta *Zabbix* e **comparações abrangentes com outras abordagens de monitoramento de redes e** será descrito, analisado e demonstrado o estudo de caso, abordando processos de instalações até a implantação do sistema virtual. Será abordada a função do *Zabbix* e a melhoria fornecida ao trabalhar em conjunto com o SNMP.

Por último, o quarto capítulo será demonstrada informações obtidas sem uso da ferramenta e descrito os resultados alcançados pelos testes após o desenvolvimento do estudo de caso, juntamente com uma análise dos dados.

# 7. CRONOGRAMA DE EXECUÇÃO

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **ETAPAS DA PESQUISA** | **Fev/2024** | **Marc/2024** | **Abr/2024** | **Maio/2024** | **Jun/2024** | **Jul/2024** |
| **Capítulo 1:** Aprofundamento bibliográfico/revisão de literatura |  |  |  |  |  |  |
| **Capítulo 2:** Explicação de conceitos da Infraestrutura e Gerenciamento de Rede e Protocolo SNMP. |  |  |  |  |  |  |
| **Capítulo 3:** Significação da ferramenta Zabbix e Implantação do Estudo de Caso. |  |  |  |  |  |  |
| **Capítulo 4:** Observação do levantamento de dados e resultados. |  |  |  |  |  |  |
| Elaboração texto do TCC |  |  |  |  |  |  |
| Revisão e validação pelo orientador |  |  |  |  |  |  |
| Defesa e entrega do TCC |  |  |  |  |  |  |

Tabela 2 - Cronograma de Execução

# 8. REFERÊNCIAS

BLACK, Tomas Lovis. **Comparação de ferramentas de gerenciamento de redes**. 2008.

FURTUNATO, Alex. **Gerência de Redes de Computadores**. Instituto Federal de Educação, Ciência e Tecnologia Rio Grande do Norte: Do Autor, 2012. 36 slides, color. Disponível em: . Acesso em: 10 agost. 2023.  
  
TANENBAUM, Andrew S. **Redes de Computadores**. 4.ed. ed. Rio de Janeiro: Campus, 2003.

HERNANTES, J.; GALLARDO, G.; SERRANO, N. **It infrastructure-monitoring tools. IEEE Software**, v. 32, n. 4, p. 88-93, 2015.

PECIALSKI, e., S., Dra., **Gerência de Redes de Computadores e de Telecomunicações**, Universidade de Santa Catarina, Florianópolis, 1999. Disponível em: . Acesso em: 28 agos. 2023.

SÊMOLA, Marcos. **Gestão da segurança da informação: uma visão executiva**. 8º ed. Rio de Janeiro, Editora Campus, 2003, 156 p.

TELECO, **Gerenciamento e Monitoramento de Rede II: Gerenciamento SNMP**, 2012. Disponível em: <http://www.teleco.com.br/tutoriais/tutorialgmredes2/pagina_2.asp>. Acesso em: 5 out. 2023.

ANTOS, S. S. N. **Monitoramento de redes: análise e configuração do software zabbix**. Trabalho de conclusão. Instituto federal de educação, ciência e tecnologia de são paulo – câmpus salto, 2015.

Silva, W., Martins, R., and Medeiros, R. (2016). **Analise e gerenciamento de redes usando uma metodologia proativa com zabbix**. HOLOS, 8:277.

WAZLAWICK, Raul Sidnei. **Metodologia de Pesquisa para Ciência da Computação**. 2. ed. Rio de Janeiro: Elsevier, 2014. 145 p. ISBN 978-85-352-7782-1.

MIRANDA, Aníbal D.A. **Introdução a Rede de Computadores.** 1º ed. Vila Velha, ES:

ESAB – Escola Superior Aberta do Brasil, 2008.

Soares, L. F., & G Colcher. (1995). **Redes de Computadores das LANs,MANs e WANs as Redes ATM** (2 ed.). Rio de Janeiro: Campus.

FERNÁNDEZ, **Rede de Computadores,** 2019.

Disponível em: https://educapes.capes.gov.br/bitstream/capes/432642/2/Livro%20%20 Redes%20de%20 Computadores.pdf. Acesso em: 5 out. 2023.

LESSA, Demian. **O Protocolo de gerenciamento RMON**. Rede Nacional de Ensino e Pesquisa (RNP), Boletim bimestral sobre tecnologia de redes, v. 3, n. 1, publicado em 15 jan. 1999. Disponível em: . Acesso em: 5 out. 2023.

HORST, Adail Spínola; PIRES, Aécio dos Santos; DÉO, André Luis Boni**. De A a Zabbix**. 1. ed. São Paulo: Novatec, 2015.

MOHIR, Rodrigo Fraga. **Análise de Ferramentas de Monitoração de Código Aberto,** 2012. Disponível em: https://lume.ufrgs.br/bitstream/handle/10183/66105/000870983.pdf. Acesso em: 9 out. 2023

1. Simple Network Management Protocolo (Protocolo Simples de Gerenciamento de Rede, tradução nossa). [↑](#footnote-ref-1)
2. Disponível em: <https://4linux.com.br/o-que-e-zabbix/>. Acesso em: 10 de ago. 2023. [↑](#footnote-ref-2)
3. É uma sequência de instruções escritas para serem interpretadas por um computador. [↑](#footnote-ref-3)
4. Software de distribuição gratuita. [↑](#footnote-ref-4)
5. Parte física do computador. [↑](#footnote-ref-5)
6. Open Systems Interconnection (Interconexão de Sistemas Abertos, tradução nossa). [↑](#footnote-ref-6)
7. International Organization for Standardization (Organização Internacional para Padronização, tradução nossa). [↑](#footnote-ref-7)
8. Um conjunto de códigos prontos que servem como estrutura para auxiliar no desenvolvimento. [↑](#footnote-ref-8)
9. Transmission Control Protocol (Protocolo de Controle de Transmissão, tradução nossa). [↑](#footnote-ref-9)
10. HyperText Transfer Protocol (Procolo de Transferência de Hipertexto, tradução nossa). [↑](#footnote-ref-10)
11. Management Information Bases (Bases de informação de gestão, tradução nossa). [↑](#footnote-ref-11)
12. Object Identifier (Identificador de Objetos, tradução nossa). [↑](#footnote-ref-12)
13. Sequências de caracteres alfanuméricos. [↑](#footnote-ref-13)
14. Service Level Agreements (Acordos de Nível de Serviço, tradução nossa). [↑](#footnote-ref-14)