UNIVERSIDADE EDUARDO MONDLANE

FACULDADE DE ENGENHARIA

DEPARTAMENTO DE ENGENHARIA ELECTROTÉCNICA

LICENCIATURA EM ENGENHARIA INFORMÁTICA – PÓS LABORAL

RELATÓRIO DE ESTÁGIO PROFISSIONAL

IMPLEMENTAÇÃO DE UM SISTEMA DE MONITORAMENTO DE REDE DE COMPUTADORES NA MERIDIAN32

Autor:

André Ezequias Comé

Supervisor da Faculdade:

Eng. Felizardo Munguambe

Supervisor da Instituição:

Eng. Víctor Guerra

Maputo, Julho de 2023

UNIVERSIDADE EDUARDO MONDLANE

FACULDADE DE ENGENHARIA

DEPARTAMENTO DE ENGENHARIA ELECTROTÉCNICA

LICENCIATURA EM ENGENHARIA INFORMÁTICA – PÓS LABORAL

RELATÓRIO DE ESTÁGIO PROFISSIONAL

IMPLEMENTAÇÃO DE UM SISTEMA DE MONITORAMENTO DE REDE DE COMPUTADORES NA MERIDIAN32

Autor:

André Ezequias Comé

Supervisor da Faculdade:

Eng. Felizardo Munguambe

Supervisor da Instituição:

Eng. Víctor Guerra

Maputo, Julho de 2023

Agradecimentos

Em primeiro lugar, agradecer a Deus pelo Dom da vida, por me abençoar e me permitir continuar lutando pelos meus sonhos.

Agradeço aos meus Pais Ezequias André Comé e Eulália Dulce Mateus que tanto lutaram para que nunca me faltasse nada, que me motivaram a seguir os meus sonhos e nunca criaram barreiras, mas sim sempre apoiaram as minhas decisões, eles foram a peça fundamental para que tudo isto fosse possível na minha vida.

Agradecer a minha namorada Maria Luísa Libombo, pelo apoio emocional e pela força que sempre me deu durante este percurso.

Agradecer ao meu supervisor, Eng.º Felizardo Munguambe, pelo apoio durante o período de estágio profissional.

A todos os docentes da Faculdade de Engenharia da UEM, em especial aos docentes do departamento da electrotécnica que contribuíram para a minha formação académica.

Por último, mas não menos importante, agradecer as minhas irmãs que foram sempre uma fonte de inspiração para mim e sempre me apoiaram incondicionalmente.

RESUMO

No mundo actual, a interconectividade proporcionada pelas redes de computadores desempenha um papel vital no funcionamento das organizações. No entanto, a complexidade e a escala dessas redes exigem uma abordagem estratégica para garantir seu bom desempenho, confiabilidade e segurança. Nesse contexto, o administrador de redes desempenha um papel crucial na manutenção e no monitoramento contínuo dessas redes. Com o objetivo de assegurar o adequado funcionamento da rede no grupo Meridian32, este trabalho propõe a implementação de um sistema de monitoramento abrangente. Através desse sistema, será possível acompanhar o desempenho dos dispositivos de rede, como servidores, switches e roteadores, bem como monitorar serviços essenciais, como a disponibilidade de serviços de rede, a integridade dos dados e a segurança da rede.

Palavras-chave: monitoramento de redes de computadores, infra-estrutura, administração de rede de computadores.

ABSTRACT

In today's world, the interconnectivity provided by computer networks plays a vital role in the functioning of organizations. However, the complexity and scale of these networks require a strategic approach to ensure their good performance, reliability and security. In this context, the network administrator plays a crucial role in the maintenance and continuous monitoring of these networks. In order to ensure the proper functioning of the network in the Meridian32 group, this work proposes the implementation of a comprehensive monitoring system. Through this system, it will be possible to track the performance of network devices such as servers, switches and routers, as well as monitor essential services such as the availability of network services, data integrity and network security.

Keywords: computer network monitoring, infrastructure, computer network administration.

ÍNDICE

1 CAPITULO I – INTODUÇÃO 1

1.1 Contextualização 1

1.2 Descrição do problema 2

1.3 Justificativa 3

1.4 Objectivos 4

1.4.1 Geral 4

1.4.2 Específicos 4

1.5 Metodologia 5

1.6 Estrutura do Trabalho 6

2 CAPÍTULO II – REVISÃO DA LITERATURA 7

2.1 Redes de computadores 7

2.1.1 Tipo de redes de computadores 7

2.2 Gerenciamento de redes de computadores 8

2.3 Monitoramento de redes de computadores 10

2.4 SNMP – Simple Network Management Protocol 11

2.5 Ferramentas de monitoramento de redes 13

2.5.1 Paessler PRTG Network Monitor 13

2.5.2 Cacti 14

2.5.3 Nagios 16

2.5.4 Zabbix 18

2.6 Critérios para selecção de uma ferramenta de monitoramento 21

2.7 Comparação de ferramentas de monitoramento 25

3 CAPÍTULO III – CASO DE ESTUDO 28

3.1 Grupo Meridian 32 28

3.2 Rede da meridian32 29

3.3 Cenário actual de monitoramento da rede na meridian32 30

3.4 Actividades realizadas no âmbito do estágio na ALTEL 31

3.4.1 Actividades em destaque 32

4 CAPÍTULO IV – IMPLEMENTAÇÃO DA SOLUÇÃO 35

4.1 Instalação do Zabbix 35

4.2 Monitoramento com Zabbix 39

5 CAPÍTULO V – CONCLUSÕES E RECOMENDAÇÕES 41

5.1 Conclusões 41

5.2 Recomendações 41

6 CAPÍTULO VI – REFERÊNCIAS BIBLIOGRÁFICAS 43

LISTA DE ABREVIATURA E ACRÓNIMOS

CPU - Central Processing Unit

CGIs - Common Gateway Interfaces

FTP - File Transfer Protocol

GPLv2 - GNU General Public License version 2

HTTP - Hypertext Transfer Protocol

IP - Internet Protocol

LLD - Low-Level Discovery

LAN - Local Area Networks

MAN - Metropolitan Area Networks

MIB - Management Information Base

NNTP - Network News Transfer Protocol

PRTG - Paessler Router Traffic Grapher

POP3 - Post Office Protocol version 3

RRD - Round Robin Database

SMTP - Simple Mail Transfer Protocol

SNMP - Simple Network Management Protocol

TI - Tecnologia de Informação

TSDB - Time Series Database

WAN - Wide Area Networks

WMI - Windows Management Instrumentation

LISTA DE FIGURAS

Figura 1 - Gerenciamento de rede, sistemas e aplicativos 9

Figura 2 - Paessler PRTG Network Monitor Interface Web 14

Figura 3 - Cacti web interface..... 15

Figura 4 - Interface padrão de monitoramento do Nagios 17

Figura 5 - Arquitectura do Zabbix..... 19

Figura 6 - Topologia de rede da Meridian32 30

Figura 7 - Criação de uma nova máquina virtual no esxi 36

Figura 8 - Configuração de IP durante o processo de instalação do ubuntu server 20.04 36

Figura 9 - Interface web da finalização da instalação do Zabbix 37

Figura 10 - Tela principal do zabbix (Dashboard)..... 37

Figura 11 - Lista de hosts monitorados pelo Zabbix..... 38

Figura 12 - log do envio de alerta por email 39

Figura 13 - Email de alerta do Zabbix 39

LISTA DE TABELAS

Tabela 1 - Requisitos de software do Cacti (Linux/Unix) 16

Tabela 2 - Tabala de requisitos de hardware para instalação do zabbix 20

Tabela 3 - Plataformas suportadas pelo zabbix 21

Tabela 4 - Comparação de ferramentas de monitoramento 26

1 CAPITULO I – INTODUÇÃO

1.1 Contextualização

No mundo actual, a necessidade de comunicação entre os seres humanos é de extrema importância para o desenvolvimento das sociedades. Um factor importante e facilitador para que essa comunicação ocorra são as redes de computadores, cujo objectivo é interligar vários computadores, cidades, países e continentes através de meios digitais.

Contemplando toda essa responsabilidade atribuída às redes de computadores, pode-se afirmar que problemas as envolvendo interferem directamente no ciclo de trabalho e evolução das sociedades, por isso, assegurar o bom funcionamento prevendo e evitando falhas é muito importante, pois assim podemos garantir a comunicação continua e o crescimento contínuo das sociedades.

Nesse contexto, o administrador de redes tem uma grande responsabilidade de assegurar os critérios de redes, segundo (Forouzan, 2007) tais critérios são, desempenho, confiabilidade e segurança.

Portanto, existem ferramentas usadas pelos administradores de redes cuja responsabilidade exclusiva é realizar de maneira precisa o monitoramento de dispositivos na rede, desde dispositivos físicos e serviços.

É nesse âmbito que o presente trabalho busca implementar um sistema de monitoramento de rede no grupo Meridian32 e também relatar as actividades desencadeadas durante o período de estágio profissional.

1.2 Descrição do problema

Com a evolução das redes de computadores, crescem também os problemas que as envolvem e a dificuldade de manter e controlar este grande sistema de comunicação, pois existem milhares de equipamentos e processos que um simples humano não poderia ser capaz de controlar sem auxílio de um sistema de monitoramento.

Nas empresas, as reclamações de processos lentos, paragem de serviços de forma repentina e diversas situações que dificultam a continuidade do negócio crescem a cada dia.

A título de exemplo, na Meridian32, a falta de um sistema de monitoramento da rede de computadores tem impossibilitado a detenção pro-activa de diversos problemas tais como: lentidão no acesso aos servidores, lentidão no acesso às aplicações como primavera, indisponibilidade de acesso a certos serviços.

Não só, o administrador de rede também não tem a visibilidade quando certos dispositivos na rede ficam desligados ou quando perdem o acesso a determinados serviços.

Face a tudo isso, até que ponto um sistema de monitoramento poderia ajudar na optimização dos serviços da rede e melhoria nos resultados nos serviços da Meridian32?

1.3 Justificativa

A escolha do tema "Implementação de um sistema de monitoramento de rede de computadores na Meridian32", surge pelo facto da empresa enfrentar diversos problemas por não possuir um sistema de monitoramento de rede que possa ajudar aos administradores a terem uma visão mais ampla dos eventos da rede e desta forma, agir de forma pro-activa na detecção de possíveis problemas. A escolha desse tema se destaca pela sua relevância e potencial para solucionar esses problemas recorrentes, uma vez que a implementação de um sistema de monitoramento pode proporcionar maior visibilidade e controle sobre a rede, possibilitando a identificação pró-activa de problemas e a tomada de acções correctivas antes que afectem os serviços oferecidos.

Outro factor relevante é o facto desta pesquisa contribuir para a minha carreira profissional criando a oportunidade de adquirir conhecimento e experiência na implementação de um sistema de monitoramento de rede de computadores. Ao me envolver nesse projeto, terei a chance de desenvolver habilidades específicas nessa área, ampliar minha expertise em tecnologias de rede e aprimorar minhas competências como administrador de redes.

Este estudo não apenas trará benefícios imediatos para a Meridian32, mas também será um fator relevante para sociedade no geral. A pesquisa pode avançar o conhecimento no campo das redes de computadores. Além disso, a pesquisa pode gerar *insights* e descobertas que possam ser aplicados em outros contextos empresariais e servir de base para futuros estudos na área de monitoramento de redes. Dessa forma, a pesquisa contribui para o avanço científico, promovendo o compartilhamento de conhecimento e a disseminação das melhores práticas no campo da tecnologia da informação.

1.4 Objectivos

1.4.1 Geral

- Implementar sistema de monitoramento de rede de computadores Zabbix na Meridian32.

1.4.2 Específicos

- Analisar o estado actual de monitoramento da rede de computadores na Meridian32;
- Descrever tarefas desempenhadas durante o estágio profissional;
- Implementar um sistema de monitoramento e monitorar a rede da Meridian32.

1.5 Metodologia

Este relatório foi elaborado com base em pesquisas bibliográficas e na consulta de recursos disponíveis na Internet. Além disso, o suporte e orientação do supervisor foram de grande importância para o desenvolvimento do trabalho.

Em relação à abordagem adoptada, optou-se pela abordagem qualitativa, a fim de aprofundar os conceitos fundamentais necessários para compreender o fenómeno em estudo. Foram analisados conceitos relacionados a sistemas de monitoramento, monitoramento de redes de computadores e a importância de monitorar a infra-estrutura de TI.

Quanto aos objectivos, este estudo é considerado exploratório, uma vez que o pesquisador realizou uma pesquisa abrangente para se familiarizar com o tema do monitoramento de redes de computadores, a fim de compreender melhor o impacto da ausência desse serviço em uma infra-estrutura de TI.

No que diz respeito aos procedimentos técnicos, o autor adoptou a análise documental, conforme proposto por Lakatos e Marconi (2003), para a revisão de revistas e artigos online, além do estudo de caso. A análise documental, como descrita por Gil (2008), envolve a utilização de materiais que não receberam tratamento analítico científico, como documentos e relatórios oficiais, que foram úteis para compreender a ocorrência do tema proposto.

1.6 Estrutura do Trabalho

O presente relatório está organizado da seguinte forma:

- **Capítulo 1 – Introdução**

  Neste capítulo, apresenta-se a contextualização do trabalho de forma a dar a entender o que se pretende arrolar, apresenta-se a descrição do problema, a justificativa, os objectivos a metodologia e por fim a estrutura do trabalho.

- **Capítulo 2 – Revisão de literatura**

  Neste capítulo, apresenta-se material bibliográfico sobre monitoramento de redes de computadores, trazendo conteúdo relevante para a selecção das melhores ferramentas de monitoramento.

- **Capítulo 3 – Caso de estudo**

  Neste capítulo, faz-se a apresentação da instituição onde decorreu o estágio profissional, descrevendo a sua composição e o cenário actual de monitoramento.

- **Capítulo 4 – Implementação da solução**

  Neste capítulo é apresenta a solução e o processo de implementação da solução.

- **Capítulo 5 – Conclusões e recomendações**

  Neste capítulo, são apresentadas as conclusões tomadas em relação ao tema.

2 CAPÍTULO II – REVISÃO DA LITERATURA

Neste capítulo, serão abordados alguns conceitos básicos relacionados a redes de computadores, gerenciamento das redes de computadores, monitoramentos e alguns sistemas de monitoramento como também destacar a sua importância.

2.1 Redes de computadores

Redes de computadores são sistemas que conectam dispositivos electrónicos, como computadores, servidores, roteadores, *switches* e dispositivos móveis, permitindo a comunicação e o compartilhamento de recursos entre eles.

As redes de computadores possibilitam a troca de informações, o compartilhamento de recursos e a comunicação entre usuários e dispositivos conectados. Além disso, elas permitem o acesso a serviços e recursos remotos, como servidores, base de dados, impressoras e dispositivos de armazenamento.

Segundo (Tanenbuam & Wetherall, 2011) redes de computadores é a colecção de computadores anonimos interconectados por uma única tecnologia. Dois computadores estão conectados se entre eles conseguem trocar informações.

As redes de computadores são implementadas nas empresas com o intuito de tornar a comunicação e partilha de dados mais fácil e eficaz, no entanto, para que as redes de computadores funcionem sem interrupção do modo a manter disponível os ficheiros compartilhados como também os serviços, é necessário que haja um trabalho de monitoramento da rede de forma a prever e prevenir possíveis problemas.

2.1.1 Tipo de redes de computadores

Existem diversos tipos de redes de computadores, cada uma com suas características e finalidades específicas. No entanto, existem 2 principais tipos de redes de computadores.

Segundo (Forouzan, 2007) actualmente quando se fala de tipos de redes, destacam-se dois tipos que podem ser locais (LANs - Local Area Networks) ou estender-se por uma área maior, como uma cidade, um país ou até mesmo o mundo (WANs - Wide Area Networks). As redes de

tamanho intermediário são normalmente chamadas de redes de área metropolitana e abrangem dezenas de quilómetros.

2.1.1.1 Local Area Network

É uma rede que abrange uma área geográfica limitada, geralmente dentro de um edifício ou campus. É utilizada para interconectar dispositivos próximos, como computadores, impressoras, servidores e dispositivos de armazenamento. As redes LAN são frequentemente usadas em empresas ou instituições educacionais. A maioria das LANs hoje são Ethernet (Vachon & Graziani, 2008).

2.1.1.2 Wide Area Network

WAN é uma rede que abrange uma área geográfica extensa em relação a LAN e geralmente usam provedoras de serviços ou telecomunicações, as WANs abrangem áreas como um país ou continente. A Internet é um exemplo de WAN (Vachon & Graziani, 2008).

2.2 Gerenciamento de redes de computadores

Para (Alexander Clemm, 2007) de uma forma simplificada, gerenciamento de redes refere-se à operacionalização da rede contando com ferramentas essenciais para suportar essas actividades, uma boa parte do gerenciamento da rede está relacionada ao monitoramento da mesma do modo a entender o seu comportamento, mas existem também outros aspectos.

De uma forma mais abrangente, (Forouzan, 2007) define gerenciamento de redes como a actividade de monitorar, configurar, testar e resolver problemas existentes nos dispositivos da rede de forma a ir de encontro com os objectivos da organização. De referir que esses objectivos estão relacionados com o bom funcionamento da rede e qualidade dos serviços para os utilizadores.

(Alexander Clemm, 2007) destaca 4 actividades principais do gerenciamento de redes:

- Operações
- Administração
- Manutenção

- Provisionamento de sistemas ou serviços

Operações - trata de manter a rede e os seu serviços activos e funcionando sem problemas. Inclui monitoramento da rede de modo a detectar problemas o mais rápido possível antes que um utilizador seja afectado pelos problemas.

Administração – envolve controlar os recursos na rede e como eles são gerenciados, tem a ver com o controle geral para manter as coisas em conformidade.

Manutenção – está relacionado com as acções necessárias, seja de reparação ou de substituição de dispositivos da rede.

Provisionamento – refere-se à configuração de recursos na rede para implementar ou suportar um novo serviço.

Salienta (Alexander Clemm, 2007) que no seu sentido mais amplo, usamos o termo gerenciamento de redes para se referir ao mundo de **gerenciamento de redes, sistemas e aplicações,** como ilustra a **figura 1**. Embora sejam por vezes distinguidos como gerenciamento de serviços, elas juntas têm muito mais em comum do que o que as separa. Salvo indicação em contrário, usamos o termo gerenciamento de rede em seu sentido mais amplo, abrangendo todas essas disciplinas intimamente relacionadas.

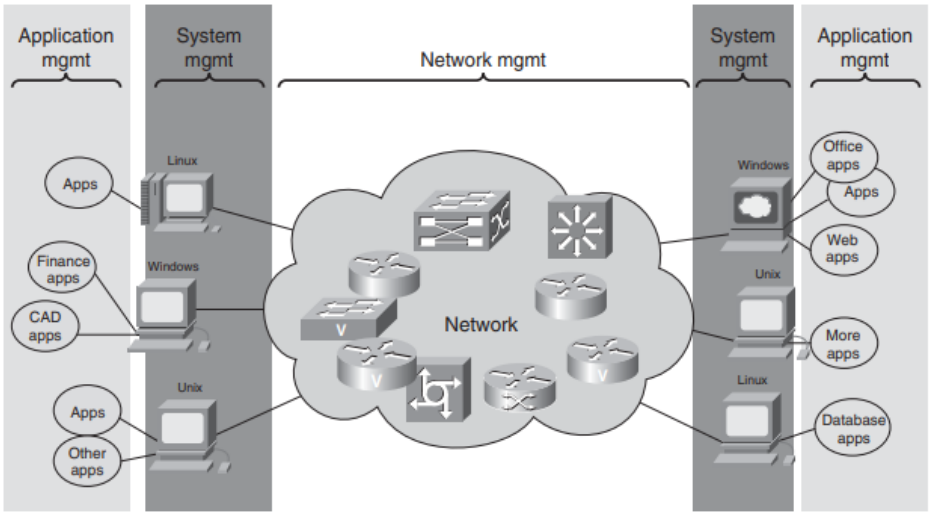

Figura 1 *- Gerenciamento de rede, sistemas e aplicativos*

Fonte: *Alexander Clemm (2007)*

2.3 Monitoramento de redes de computadores

É visto que o monitoramento é uma boa parte do gerenciamento das redes de computadores como afirmado por (Alexander Clemm, 2007).

Podemos desta forma afirmar que o monitoramento surgiu com a necessidade de detectar possíveis problemas em uma rede de forma pro-activa e consequentemente tomar medidas antes que pudesse acontecer um possível desastre.

O monitoramento é actualmente uma tarefa indispensável independentemente da dimensão da rede, uma rede sem monitoramento não tem como se manter operacional por muito tempo principalmente quanto maior for pois o controle humano limita-se cada vez mais que essa rede vai crescendo.

O monitoramento de redes de computadores é essencial para garantir o bom funcionamento e desempenho da sua infra-estrutura de rede. Ao monitorar o tráfego de rede, os administradores podem identificar gargalos, optimizar o uso da largura de banda e melhorar a qualidade dos serviços. Além disso, o monitoramento contínuo permite a detecção de erros e falhas, permitindo uma resposta rápida e eficiente para minimizar o tempo de inactividade e manter os serviços disponíveis aos utilizadores.

Nessa perspectiva, (Durieux, 2012) afirma que a ideia principal do monitoramento é fornecer ao administrador de redes ferramentas para que ele esteja apto a monitorar equipamentos remotos, analisar os dados de modo que funcionem nos limites especificados. Controlar pro-activamente o sistema, detectar anomalias e e corrigir antes que torne-se em um problema mais sério.

Ainda Segundo (Durieux, 2012) o monitoramento de redes tem a função de prover dados e ferramentas para auxiliar o administrador de redes na execução de três actividades a seguir:

1. **Dimensionamento da infra-estrutura de TI:**

   Consta na lista dos problemas mais complicados de serem resolvidos, o monitoramento traz dados tais como atraso na entrega, disponibilidade dos serviços, entre outros factores importantes na determinação do que alterar para melhor desempenho. Um

exemplo seria uma empresa lançando um serviço de venda pela internet, se não for feito o dimensionamento correcto, os utilizadores não poderão efectuar as compras devido a demanda pelo facto de ser um lançamento novo e desta forma podemos afirmar que o sucesso é directamente proporcional ao desempenho do sistema.

2. **Segurança:**

   Neste âmbito, o monitoramento pode fornecer registos que podem ajudar a detectar actividades incomuns na rede ajudando a agir de forma pro-activa e evitar problemas graves.

3. **Caracterização do tráfego:**

   A caracterização do tráfego pode ajudar o administrador a saber qual serviço é mais utilizado na rede, um exemplo poderia ser separar o tráfego por serviços (HTTP, FTP, SMTP) do modo a dimensionar de forma correcta o sistema.

2.4 SNMP – Simple Network Management Protocol

No início da era das redes de computadores, identificar problemas nos componentes de rede era uma tarefa relativamente simples devido ao tamanho reduzido das redes. No entanto, à medida que as redes cresceram e mais dispositivos foram interligados, surgiu a necessidade de estabelecer uma estrutura que facilitasse o controle e o gerenciamento desses dispositivos em conjunto (Cadorin, 2003).

Ainda segundo (Cadorin, 2003) alega que apesar de várias tentativas anteriores de criar ferramentas de gerenciamento mais eficazes, nenhuma delas obteve sucesso. Foi então que surgiu a RFC 1157, que definiu a primeira versão do SNMP (Simple Network Management Protocol). Essa solução revolucionária tornou o gerenciamento de redes mais fácil e otimizado, facilitando o trabalho dos administradores. Como resultado, o SNMP rapidamente se tornou um padrão amplamente adoptado para o gerenciamento de redes, com diversos fabricantes incorporando-o em seus produtos.

No entanto, à medida que o uso do SNMP se expandiu, começaram a surgir falhas no projeto original do SNMPv1. Diante disso, uma nova versão, conhecida como SNMPv2, foi desenvolvida para corrigir as deficiências encontradas, especialmente no que diz respeito à segurança do protocolo. Essa nova versão do SNMP se tornou um padrão amplamente aceito na comunidade de redes, embora posteriormente tenha sido lançada a versão SNMPv3, que introduziu recursos avançados de segurança, como a criptografia na comunicação entre o agente e o gerente (Cadorin, 2003).

A evolução contínua do SNMP ao longo do tempo demonstra o compromisso em aprimorar as soluções de gerenciamento de redes, visando garantir a segurança e a eficiência no monitoramento e controle dos dispositivos interconectados.

Segundo (Eler, 2015) o modelo SNMP e a maioria dos sistemas de gerenciamento são baseados no modelo Agente/Gerente, que envolve os seguintes componentes:

- **Agente:** é um programa executado nos dispositivos que serão gerenciados. Sua função é responder às solicitações do Gerente e gerar mensagens sempre que ocorrer uma alteração de status em um objecto específico.

- **Gerente:** é um programa executado em um elemento de rede que actua como intermediário entre o utilizador final e o sistema de gerenciamento. Ele converte as solicitações do utilizador em acções que serão executadas na rede.

- **Protocolo de Gerenciamento:** é o protocolo utilizado para padronizar a troca de informações entre o Gerente e o Agente. Ele é o elemento central de uma rede de gerenciamento. Essa troca de informações pode ocorrer de duas maneiras: através de interacções de comando/resposta, em que o Gerente faz uma solicitação e o Agente responde, ou por meio do envio de informações do Agente para o Gerente sem uma solicitação prévia, conhecido como mensagens do tipo TRAP.

- **MIB** (Management Information Base): é uma base de dados localizada no Agente que contém informações e estruturas dos objectos que podem ser gerenciados pelo Gerente. Esses objectos podem incluir, por exemplo, interfaces seriais ou fontes em um roteador.

2.5 Ferramentas de monitoramento de redes

Ao tomar a decisão de escolher uma ferramenta de monitoramento de rede, os administradores de rede são confrontados com um desafio significativo. Actualmente, o mercado oferece uma ampla variedade de mais de 50 ferramentas fornecidas por diferentes provedores. Embora essas ferramentas ofereçam uma ampla gama de possibilidades, é importante reconhecer que existem diferenças distintas entre elas que podem desempenhar um papel crucial no contexto da rede (Shokhin, 2015).

Serão apresentadas algumas ferramentas de monitoramento mais populares no mercado, e uma comparação das mesmas.

2.5.1 Paessler PRTG Network Monitor

Uma das principais vantagens desse produto é sua usabilidade. Ele pode ser instalado com apenas alguns cliques e possui um recurso de auto-descoberta que permite fazer o *scan* da rede e adicionar automaticamente elementos para monitoramento. Além disso, o PRTG não apenas oferece uma interface web amigável, mas também uma versão desktop e aplicativos móveis para iOS e Android, permitindo monitoramento em movimento. Isso significa que os administradores de rede podem acompanhar o status e receber notificações importantes mesmo quando estão longe do escritório.

O PRTG Network Monitor oferece recursos abrangentes, incluindo monitoramento em tempo real, gráficos intuitivos e relatórios detalhados como ilustra a **figura 2**. Ele permite que os administradores monitorem a disponibilidade de dispositivos, verifiquem o desempenho da rede, analisem o tráfego de dados e monitorem aplicativos críticos. Com uma interface intuitiva e recursos avançados, o PRTG torna mais fácil para os administradores identificarem e solucionarem problemas de rede, garantindo a estabilidade e o bom funcionamento do ambiente de rede (King, 2023).

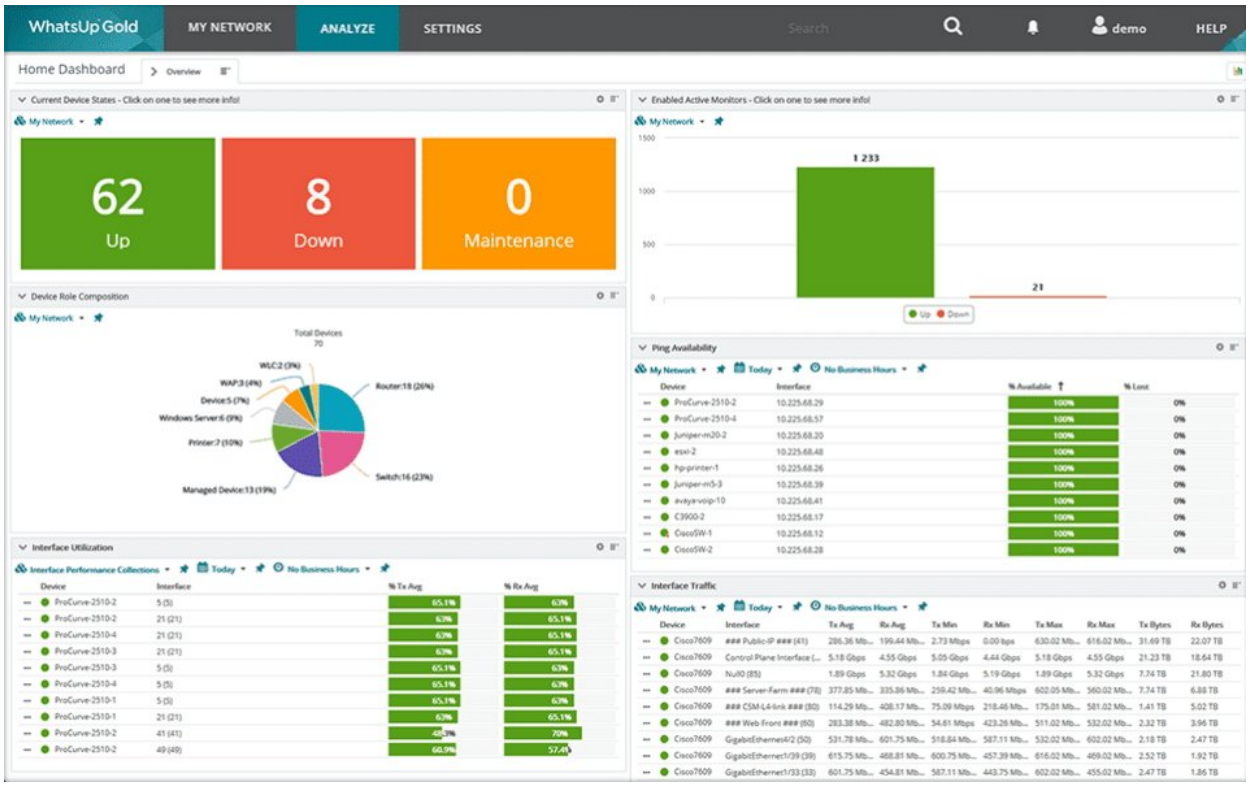

Figura 2 *- Paessler PRTG Network Monitor Interface Web*

Fonte: *Network King (2023)*

2.5.2 Cacti

O cacti é uma estrutura robusta de gerenciamento de desempenho e falhas e uma interface para o RRDTool - um Banco de Dados de Séries Temporais (TSDB). Ele armazena todas as informações necessárias para criar gráficos de gerenciamento de desempenho no MariaDB ou MySQL e, em seguida, utiliza seus diversos coletores de Dados para preencher o TSDB baseado no RRDTool com esses dados de desempenho (Cacti, n.d.).

O Cacti (**figura 3**) permite acompanhar uma variedade de métricas, como a quantidade de memória utilizada, o número de processos em execução, a quantidade de utilizadores conectados, o tráfego de entrada e saída, entre outros, que podem variar de acordo com o tipo de dispositivo. Essas informações são plotadas em gráficos ao longo do tempo, permitindo análises sobre os horários de maior actividade e auxiliando no dimensionamento da carga. É uma forma de obter *insights* sobre o desempenho e a utilização dos dispositivos monitorados (Yano, 2010).

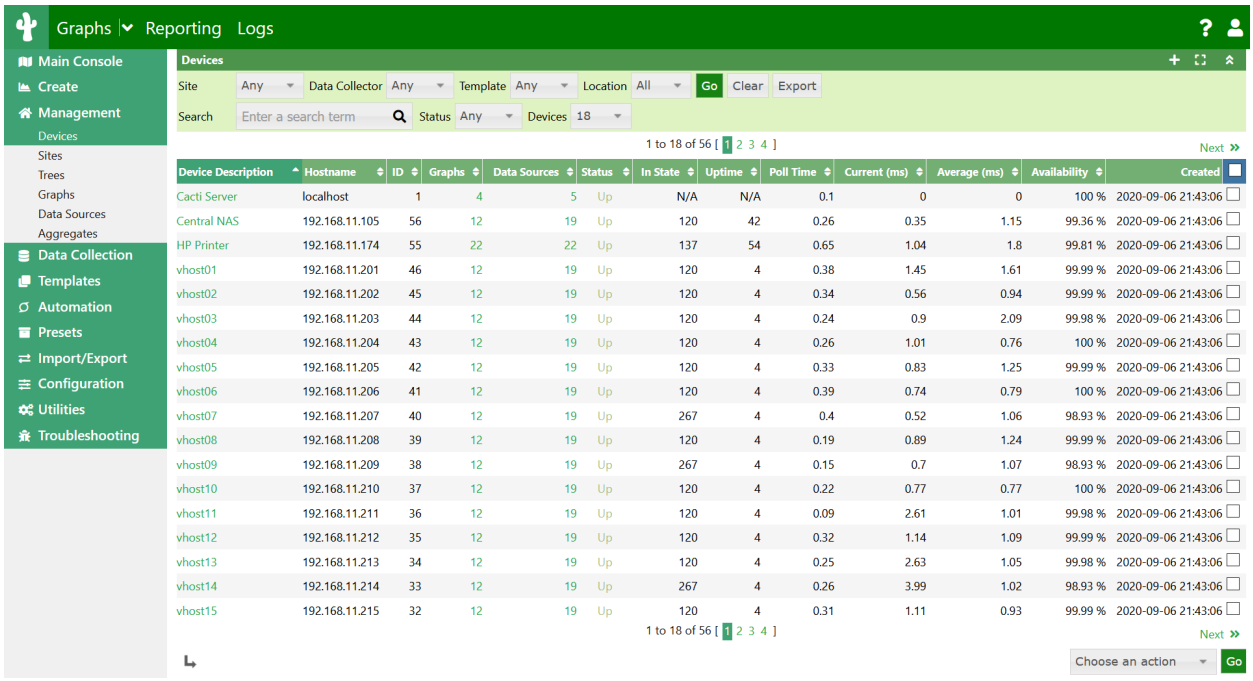

Figura 3 *- Cacti web interface*

Fonte: *(Cacti, n.d.)*

Alguns recursos do Cacti segundo (Andreoli, 2016):

Gráficos: O Cacti oferece um número ilimitado de gráficos que podem ser configurados em diferentes formatos, como gráficos de área, linha, barra, entre outros. Além disso, ele permite ao administrador personalizar cores, legendas e outros detalhes para facilitar a visualização dos gráficos.

Coleta de dados: O Cacti permite que os usuários coletem dados por meio de scripts externos e também oferece suporte ao protocolo SNMP, permitindo a obtenção de informações de dispositivos de rede.

Gerenciamento de utilizadores: O Cacti possibilita que o administrador crie utilizadores e aplique regras de permissão a eles. Isso permite controlar o acesso e as funcionalidades disponíveis para cada usuário no sistema.

Requisitos do software

O Cacti foi desenvolvido para ser executado em sistemas operacionais baseados em Unix/Linux, como Ubuntu, CentOS, Debian, entre outros. No entanto, com o avanço da tecnologia e a

disponibilidade de ferramentas e pacotes adicionais, é possível instalar o Cacti em outros sistemas operacionais, incluindo o Windows.

A tabela abaixo **(tabela 1)**, mostra os requisitos para a instalação do Cacti no Linux/Unix (Bezerra, 2015).

SISTEMA	VERSÃO	COMENTÁRIOS
RRDTool	1.0.49 ou 1.2.x/superior	
MySQL	4.1.x ou 5.x/superior	
PHP	4.3.6/superior ou 5.x/superior	A versão 5.x é recomendada por suas funcionalidades avançadas
Apache	2.0 ou superior	

Tabela 1 - *Requisitos de software do Cacti (Linux/Unix)*

Fonte: *(Bezerra, 2015)*

2.5.3 Nagios

Nagios é uma solução de monitoramento de código aberto baseada em Linux, é usada para monitorar máquinas, dispositivos e serviços, a ferramenta vem equipada de uma *interface web* **(figura 5)** que permite que os administradores acessem informações críticas de monitoramento, revisem alertas, gerenciem configurações e visualizem o status dos dispositivos e serviços monitorados. Embora possa não ser a interface mais moderna ou esteticamente agradável, ela fornece as funcionalidades necessárias para o gerenciamento e monitoramento eficazes da rede.

O Nagios é um sistema de monitoramento poderoso que permite que as organizações identifiquem e resolvam problemas na infra-estrutura de TI antes que eles afectem os processos de negócios críticos (Nagios, n.d.).

O Nagios oferece as funcionalidades básicas de alerta e notificação comuns a outras ferramentas de monitoramento de rede. Recursos de alerta mais avançados estão disponíveis por meio de complementos adicionais. No entanto, se você valoriza *interfaces* de utilizador e painéis de controle visualmente atraentes, o Nagios pode não ser a opção ideal, pois sua *interface web* é considerada antiquada e pouco intuitiva (King, 2023).

Além da versão gratuita (Nagios Core), existem duas edições comerciais da Nagios IX. Essas edições podem ser interessantes se você procura uma configuração com menos trabalho manual, pois oferecem assistentes de configuração, recursos avançados de visualização e relatórios, além de painéis de controle personalizados (King, 2023).

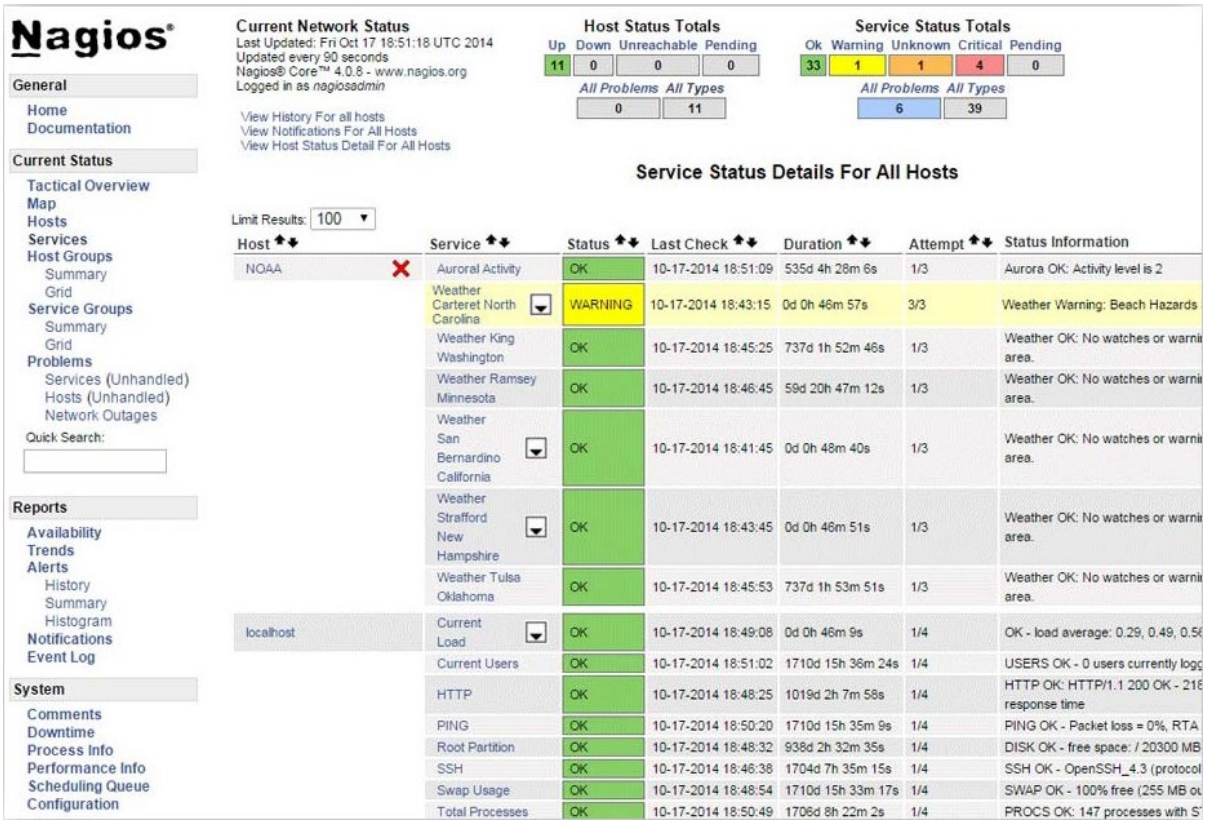

***Figura 4** - Interface padrão de monitoramento do Nagios*

***Fonte:** (Nagios, n.d.)*

Características do Nagios Core

O Nagios possui várias características que o tornam uma ferramenta popular e amplamente utilizada para o monitoramento de redes. Algumas das principais características do Nagios incluem:

- Monitoramento de serviços de rede (SMTP, POP3, HTTP, NNTP, PING, etc.)
- Monitoramento de recursos do *host* (carga do processador, uso do disco, etc.)
- Design de plugins simples que permitem aos utilizadores desenvolver facilmente seus próprios *checks* de serviços

- Notificações quando ocorrem e são resolvidos problemas de serviço ou *host* (por e-mail, ou método definido pelo utilizador)

- Capacidade de definir manipuladores de eventos a serem executados durante eventos de serviço ou *host* para resolução pro-activa de problemas

- Suporte para implementar *hosts* de monitoramento redundantes

- Interface web opcional para visualizar o status actual da rede, histórico de notificações e problemas, arquivo de log, etc. (Core, n.d.).

Requisitos para instalação do Nagios Core

O único requisito para executar o Nagios Core é uma máquina com Linux (ou uma variante UNIX) que tenha acesso à rede e um compilador C instalado (se estiver instalando a partir do código-fonte). Você não é obrigado a usar os CGIs incluídos no Nagios Core. No entanto, se você decidir usá-los, precisará ter um servidor web (preferencialmente o Apache) e ter a biblioteca gd de Thomas Boutell, versão 1.6.3 ou superior (Core, n.d.).

2.5.4 Zabbix

Zabbix é uma ferramenta de monitoramento de rede que realiza o monitoramento centralizado da disponibilidade e desempenho da rede e dispositivos de rede. Em caso de falha, um alerta é enviado para notificar um administrador de rede por telefone ou e-mail. O Zabbix é uma ferramenta de monitoramento de rede totalmente gratuita, lançada sob a licença GPLv2. Não há limitações em termos de capacidades e número de dispositivos monitorados. É permitido fazer modificações no nível do código-fonte. Além disso, o Zabbix suporta qualquer tamanho de instalação de rede: pode ser uma rede de pequeno porte ou até mesmo uma arquitectura de nível empresarial. A equipe do Zabbix lança regularmente melhorias e actualizações (Shokhin, 2015).

Arqutectura do Zabbix

O Zabbix é composto por várias partes que desempenham funções específicas no monitoramento. Temos o Zabbix Server, Zabbix Proxy, Zabbix Agent e a Interface Web (Shokhin, 2015).

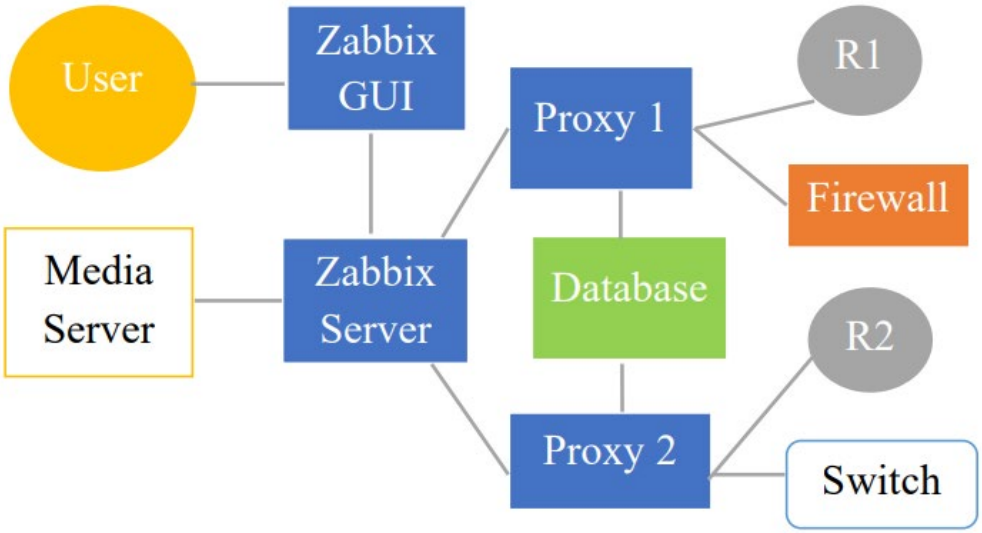

Figura 5 *- Arquitectura do Zabbix*

Fonte: *(Shokhin, 2015)*

O **Zabbix Server** é a parte central do Zabbix. Seu principal objetivo é realizar o monitoramento remoto da rede e de seus componentes. Além disso, ele armazena configurações, dados históricos e operacionais. Em caso de erro, o Zabbix Server enviará um alerta ao administrador de rede (Zabbix, 2014 como citado em Shokhin, 2015).

O **Zabbix Proxy** coleta o desempenho dos dados em nome do Zabbix Server. No nível local, todos os dados são coletados em um *buffer* que será encaminhado ao Zabbix Server. O Proxy é a solução para o monitoramento remoto centralizado da rede. Além disso, o Proxy distribui a carga de trabalho do Zabbix Server, reduzindo o consumo de recursos de CPU e memória (Zabbix, 2014 como citado em Shokhin, 2015).

O **Zabbix Agent** realiza o monitoramento local dos dispositivos de rede. Ele monitora recursos como disco rígido, memória e estatísticas da CPU. Para realizar o monitoramento de recursos, o Zabbix Agent deve ser instalado localmente em cada dispositivo. O Zabbix Agent é altamente eficaz, pois faz chamadas de sistema nativas para colectar dados estatísticos (Zabbix, 2014 como citado em Shokhin, 2015).

A **Interface Web** faz parte do Zabbix Server e geralmente é executada no mesmo servidor físico onde o Zabbix Server está rodando. A *Interface Web* não é a interface tradicional. Todas as operações de leitura e gravação são direcionadas ao banco de dados, contornando o Zabbix

Server. Isso melhora significativamente o desempenho do Zabbix. Por outro lado, o Zabbix Server não funciona sem a Interface Web (Zabbix, 2014 como citado em Shokhin, 2015).

Na **figura 5** tem dois itens adicionais que apesar de não terem sido mencionados acima, desempenham um papel importante no monitoramento da rede. O **media server** é responsável por mandar notificações e a **base de dados (data base)** é responsável pelo armazenamento das configurações e históricos (Zabbix, 2014 como citado em Shokhin, 2015).

Requisitos para instalação

O Zabbix tem requisitos de recursos de hardware que dependem do tamanho da infraestrutura a ser monitorada. Recomenda-se ter memória RAM suficiente para acomodar a carga de trabalho do Zabbix e espaço em disco adequado para armazenar os dados de monitoramento (Zabbix LLC, 2021).

A **tabela 2** especifica uma margem a considerar quando se planeia instalar o Zabbix.

Tamanho da instalação	Métricas monitorizadas	Núcleos de CPU/vCPU	Memória (GiB)	Base de dados
Pequena	1000	2	8	MySQL Server, Percona Server, MariaDB Server, PostgreSQL
Média	10000	4	16	MySQL Server, Percona Server, MariaDB Server, PostgreSQL
Grande	100000	16	64	MySQL Server, Percona Server, MariaDB Server, PostgreSQL
Muito grande	1000000	32	96	MySQL Server, Percona Server, MariaDB Server, PostgreSQL

Tabela 2 - *Tabala de requisitos de hardware para instalação do zabbix*

***Fonte**: (Zabbix LLC, 2021)*

Nota: 1 Métrica = 1 *item* + 1 *trigger* + 1 Gráfico

Plataformas suportadas

Devido aos requisitos de segurança e à natureza de missão crítica do servidor de monitoramento, o UNIX é o único sistema operacional que pode fornecer consistentemente o desempenho, a tolerância a falhas e a resiliência necessários (Zabbix LLC, 2021).

O Zabbix opera em versões líderes de mercado. Os componentes do Zabbix estão disponíveis e testados para as plataformas na **tabela 3**.

Plataforma	Servidor zabbix	Agente	Agente 2
Linux			
IBM AIX			
FreeBSD			
NetBSD			
OpenBSD			
HP-UX			
Mac OS X			
Solaris			
Windows			

***Tabela 3** - Plataformas suportadas pelo zabbix*

***Fonte**: (Zabbix LLC, 2021)*

2.6 Critérios para selecção de uma ferramenta de monitoramento

Existem algumas diferenças que podem desempenhar um papel importante na rede. Por isso, para escolher a melhor opção para a rede de uma empresa, algumas características importantes devem ser analisadas (Shokhin, 2015).

Shokhin destaca os seguintes critérios:

- **Proprietário vs código aberto**

Actualmente, existem dois tipos de aplicativos de monitoramento disponíveis no mercado. O primeiro é uma ferramenta de monitoramento com código aberto. Geralmente, esses sistemas são lançados sob a licença GPLv2. Isso significa que desenvolvedores terceiros têm permissão para fazer alterações no código. O segundo tipo são ferramentas proprietárias de monitoramento. A licença restringe qualquer tipo de modificação no código.

Na perspectiva de (Shokhin, 2015) o monitoramento de rede de código aberto traz consideravelmente mais vantagens em comparação com as soluções proprietárias. O utilizador final se beneficia com a quantidade de recursos oferecidos pelos sistemas abertos.

Apesar de os fornecedores de ferramentas de monitoramento de rede tentarem incluir os recursos mais relevantes, é quase impossível criar uma solução que seja ideal para qualquer rede. Diferentes redes têm necessidades diferentes. É aí que as ferramentas de monitoramento de rede de código aberto têm suas vantagens. Se algum recurso relevante para o monitoramento de rede não estiver incluído na versão padrão, com habilidades e conhecimentos suficientes, ele pode ser criado pelo administrador de rede ou baixado da comunidade.

- **Com base em agente vs sem agente**

Uma outra decisão para os administradores de sistemas é escolher se o monitoramento de rede deve ser feito por meio de agentes ou sem a necessidade deles. Não existe uma solução ótima única para todas as redes. Isso depende do nível de monitoramento desejado, do tipo de rede e até mesmo do orçamento disponível. Por isso, é importante compreender as diferenças principais entre essas abordagens, a fim de escolher a melhor solução para a rede da empresa.

O benefício-chave do monitoramento baseado em agente é que ele oferece análises mais aprofundadas da rede. Além disso, as ferramentas de monitoramento baseadas em agente podem até diagnosticar o desempenho do hardware. Elas também oferecem recursos de alerta e relatórios. Alguns problemas podem ser automaticamente identificados e resolvidos (EG, 2013 como citado em Shokhin, 2015).

A principal desvantagem é que a implantação desse tipo de sistema é um processo que consome tempo, pois requer a consideração de muitos detalhes da rede. Além disso, é necessário atualizar os agentes regularmente. A solução tradicional baseada em agentes pode afetar o desempenho da rede. Também é importante levar em conta que as ferramentas de monitoramento baseadas em agentes têm um custo de licença consideravelmente mais alto (Uptime Software Inc., 2014 como citado em Shokhin, 2015).

A abordagem sem agente é uma solução que não requer a instalação de agentes adicionais. A análise da rede é realizada diretamente monitorando os pacotes de dados. Essa abordagem é utilizada para monitorar a disponibilidade e o desempenho da rede. No entanto, ela não fornece informações detalhadas sobre as falhas.

O monitoramento sem agente geralmente é baseado em protocolos como SNMP (Simple Network Monitoring Protocol) ou WMI (Windows Management Instrumentation). Ele é realizado por meio de uma estação central de gerenciamento que monitora todos os dispositivos de rede (Uptime Software Inc., 2014 como citado em Shokhin, 2015).

A principal vantagem de usar o monitoramento sem agente é a eliminação da necessidade de instalar um agente separado. Isso significa que não há impacto no desempenho da rede. Além disso, o processo de implantação é mais simples e não é necessário atualizar regularmente o agente. Além disso, o custo geralmente é mais baixo. A maior desvantagem do monitoramento sem agente é a falta de métricas detalhadas. Além disso, o monitoramento sem agente não oferece recursos de relatórios ou análises avançadas (EG, 2013 como citado em Shokhin, 2015).

- **Descoberta automática**

Descoberta automática permite descobrir novos dispositivos na rede sempre que são conectados, isso é muito útil principalmente em redes grandes, podendo facilitar o trabalho do administrador de redes.

A descoberta automática é um recurso que permite realizar uma busca de elementos de rede. Além disso, ela adiciona automaticamente novos dispositivos e remove aqueles que não fazem mais parte da rede. Também realiza a descoberta de interfaces de rede, portas e sistemas de arquivos (Zabbix, 2015 como citado em Shokhin, 2015).

- **Descoberta de baixo nível**

A Descoberta em Baixo Nível (LLD) é usada para monitorar sistemas de arquivos e interfaces de rede sem a necessidade de criar e adicionar manualmente cada elemento. A descoberta em baixo nível é um recurso dinâmico que adiciona e remove elementos automaticamente. Além disso, ela cria automaticamente gatilhos e gráficos para sistemas de arquivos, interfaces de rede e tabelas SNMP (Zabbix, 2013 como citado em Shokhin, 2015).

Antes da adoção generalizada da Descoberta de Baixo Nível (LLD), os modelos de template eram amplamente utilizados. No entanto, criar um template era um processo demorado e tedioso para os gerentes de rede. Cada porta ou disco lógico exigia a criação manual de um gatilho específico, e era necessário especificar o que o gatilho deveria monitorar. Por exemplo, em uma rede com um switch de 24 portas, era preciso criar até 14 elementos diferentes usando SNMPv2 e gatilhos IF-MIB. Além disso, copiar e distribuir esses templates para todos os dispositivos de rede adicionais exigia ainda mais tempo e esforço (Zabbix Blog, 2013 como citado em Shokhin, 2015).

- **Previsão de tendências**

Algumas ferramentas de monitoramento de rede possuem um recurso chamado de previsão de tendências. Esse recurso é utilizado para detectar falhas antes mesmo de ocorrerem. Para isso, são coletados dados sobre a largura de banda da rede e o status dos dispositivos sob carga normal de trabalho. Todas as informações são armazenadas em um banco de dados SQL. Em seguida, os resultados do monitoramento são comparados às informações armazenadas no banco de dados. Se forem identificadas alterações nos dados, o sistema de monitoramento gera um alerta. Dessa forma, é possível agir preventivamente e antecipar potenciais problemas na rede (Shokhin, 2015).

- **Agrupamento lógico**

  Em redes grandes, compostas por muitos dispositivos, é difícil monitorar e solucionar problemas em todos os dispositivos durante o monitoramento dinâmico da rede. A agrupação lógica permite combinar dispositivos do mesmo tipo. Como resultado, a agrupação lógica torna o monitoramento de redes de nível empresarial significativamente mais fácil (Shokhin, 2015).

  A agrupação lógica permite combinar dispositivos de rede do mesmo tipo em grupos. Para cada grupo, pode-se definir o que deve ser monitorado e quais ações devem ser realizadas em caso de falha. Além disso, com o uso da agrupação lógica, é possível fazer configurações unificadas para todos os membros do grupo. Se um ou mais membros do grupo estiverem inativos ou offline, um alerta é exibido (Shokhin, 2015).

  Em resumo, a agrupação lógica fornece ajuda adicional aos administradores de sistemas no monitoramento do status dos dispositivos. Quase todas as ferramentas de monitoramento de rede atuais fornecem a opção de agrupamento lógico (Shokhin, 2015).

2.7 Comparação de ferramentas de monitoramento

Com base nos critérios apresentados por Shokhin, é apresentada uma comparação das ferramentas de monitoramento na **tabela 4**.

Critéiros / **Ferramenta**	**Paessler PRTG Network Monitoring**	**Cacti**	**Nagios**	**Zabbix**
Proprietário	Sim	Não	Não	Não
Código aberto	Não	Sim	Sim	Sim
Com agente	Sim	Sim	Sim	Sim
Sem agente	Sim	Sim	Sim	Sim
Descoberta automática	Sim	Não	Não	Sim

Descoberta de baixo nível	Sim	Não	Não	Sim
Previsão de tendências	Sim	Não	Não	Sim
Agrupamento lógico	Sim	Sim	Sim	Sim

***Tabela 4** - Comparação de ferramentas de monitoramento*

Fonte: Elaborado pelo autor

Com base na comparação realizada entre as ferramentas Zabbix, Cacti, Nagios e PRTG, e informações adicionais sobre as ferramentas, foram identificadas algumas constatações. O Zabbix, sendo uma ferramenta de código aberto, oferece uma ampla gama de recursos e flexibilidade, além de ser altamente escalável. Ele possui recursos avançados de automação e personalização, o que o torna uma opção interessante para organizações que desejam um alto grau de controle e adaptação.

O Cacti, também uma ferramenta de código aberto, oferece uma interface amigável e intuitiva, permitindo a criação de gráficos de desempenho e monitoramento de rede. Ele é especialmente adequado para monitorar o tráfego de rede e possui uma comunidade activa que contribui com plugins e modelos pré-configurados.

O Nagios, uma ferramenta de código aberto, possui uma longa história e é amplamente utilizado na comunidade de monitoramento de rede. Ele oferece recursos abrangentes de monitoramento e alerta, permitindo a detecção pro-activa de problemas. O Nagios requer a configuração manual de hosts e serviços, mas sua robustez e flexibilidade o tornam uma opção sólida para muitas organizações.

O PRTG, por outro lado, é uma solução proprietária que oferece uma interface amigável e intuitiva. Ele é conhecido por sua facilidade de instalação e configuração, tornando-se uma opção atraente para organizações que desejam uma solução pronta para uso. O PRTG suporta uma ampla variedade de dispositivos e oferece recursos avançados, como previsão de tendências e relatórios detalhados.

Em resumo, a escolha da solução dessas ferramentas depende da necessidade específica de cada empresa, tendo em conta o facto da organização em que decorrem os estudos estar a

procura de uma solução robusta com custos baixos de instalação, o Zabbix se mostra uma ótima opção. A possibilidade de detecção automática de dispositivos como também o facto de existirem diversas informações na internet em relação a ferramenta, sem contar com a documentação disponibilizada pela Zabbix, faz desta ferramenta uma óptima opção para implementação na rede em estudo.

3 CAPÍTULO III – CASO DE ESTUDO

Neste capítulo faz-se a descrição do grupo Meridian32, visto que é nessa instituição onde decorrem os eventos dos quais são abordados neste relatório.

Considerando o facto da Meridian32 ser uma *holding*, será sintetizada a descrição das demais empresas com foco na ALTEL onde o autor fez o seu estágio profissional. O caso de estudo é exactamente o grupo Meridian32, a ALTEL é a empresa responsável por administrar a rede de computadores da Meridian32.

3.1 Grupo Meridian 32

O grupo Meridian32 é uma incubadora de negócios, ela é constituída por diversas empresas que actuam em diferentes áreas no mercado:

- **REC (Real Estate Consulting):** especializada em estudos de mercado, estudos de viabilidade e avaliações de activos. Também desenvolve projectos de engenharia, arquitetura e gestão de projectos.

- **Zambujo & Associados:** dedica-se à inventariação, reconciliação e valoração de imóveis, equipamentos, frotas e maquinaria.

- **Predial:** actua no ramo da mediação imobiliária, auxiliando os clientes na aquisição, venda ou arrendamento de imóveis.

- **JA:** oferece serviços de gestão de instalações, venda, montagem e manutenção de geradores, ar condicionado e equipamentos diversos. Também realiza reabilitação e remodelação de espaços.

- **Fantoffice:** especializada em soluções completas para escritórios, fornecendo equipamentos para hotéis, clínicas e espaços comerciais. Destaca-se no fornecimento de mobiliário, sistemas de divisórias, estores e alcatifas.

- **Serenus:** actua no sector de segurança privada, com serviços como protecção patrimonial, segurança pessoal, guarda-costas, segurança electrónica e monitoramento de alarmes.

- **Incentea:** presta serviços profissionais nas áreas de Tecnologias de Informação e Comunicação, Inovação, Consultoria de Negócio e Engenharia de Produto. É o maior representante dos produtos Primavera em Moçambique.

- **WidePartner:** implementa sistemas de informação ERP em várias áreas de actividade, como produção, distribuição, varejo e serviços, utilizando produtos da SAGE.

- **AccSys:** oferece serviços de auditoria, contabilidade, fiscalidade, outsourcing, consultoria de gestão e implementação de sistemas de gestão com certificação ISO**.**

- **Amb&Veritas:** especializada em consultoria ambiental, aspectos sociais e formação em higiene e segurança no trabalho, utilizando a marca NOSA.

- **ALTEL Soluções Globais de Comunicação:** empresa tecnológica especializada em integração de Tecnologias de Informação, Segurança Electrónica e Radio Transmissão. Tem parcerias com empresas renomadas mundialmente.

A ALTEL proveniente da antiga ALCATEL Moçambique é uma empresa moçambicana de Tecnologia da Informação e Comunicações (TIC). Fundada há 20 anos, a ALTEL tem como objetivo desenvolver, evoluir e transformar o setor de TIC em Moçambique, em parceria com a Regra, S.A., uma empresa portuguesa de destaque no mercado de tecnologia.

A ALTEL é responsável pela infra-estrutura informática do grupo meridian32, actuando como o centro de TI no grupo, a ALTEL é responsável pelo suporte interno, administração dos sistemas e dos serviços da rede como também responsável pelo sistema de segurança electrónico implementado na Meridian32.

3.2 Rede da meridian32

Grupo Meridian32 possui uma infra-estrutura informática partilhada entre as diversas empresas pertencentes ao grupo com excepção das empresas Serenus e JA que possui infra-estrutura autónoma e independente. Das 11 empresas acima apresentadas apenas 8 delas pertencem ao mesmo escritório de trabalho nomeadamente Accsys, ALTEL, Ambveritas, Fantoffice, Incentea, Predial, REC, Zambujo & Associados e fazem uso da mesma infra-estrutura informática administrada pela ALTEL.

A topologia de rede da meridian32 como ilustra a **figura 6**, é composta por 1 firewall responsável por interligar a rede LAN com a internet, um Switch de camada 3 (Layar 3) que faz o processamento principal interligando os demais equipamentos da rede como os servidor blade que aloja as máquinas virtuais, e os demais switches usados para distribuir o sinal para os restantes dispositivos da rede como access point's (pontos de acesso) e workstations.

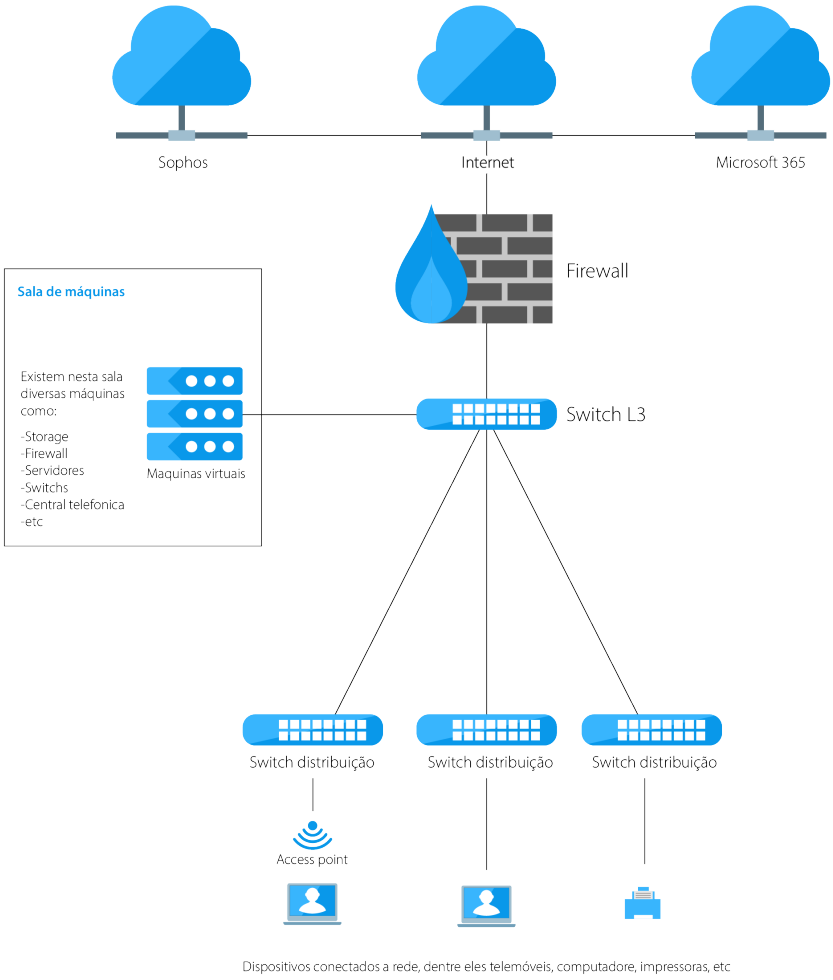

***Figura 6** - Topologia de rede da Meridian32*

***Fonte:** Elaborado pelo autor*

3.3 Cenário actual de monitoramento da rede na meridian32

Actualmente, o monitoramento é feito de forma manual ou ocasional, não existe uma política de monitoramento implementado, assim sendo, geralmente um dispositivo é só controlado após ele apresentar certas anomalias, esse controle é feito através de *logs*. O administrador da

rede é responsável por extrair os *logs* com o intuito de perceber as causas do problema detectado.

Quanto aos servidores como *file share*, onde o controle do armazenamento é importante do modo controlar o espaço disponível em rede. O controle é feito manualmente observando o espaço em disco pelo drive mapeado nos computadores ou acessando directamente ao servidor.

Quanto ao servidor físico, neste caso o *blade server* onde roda o VMware, o Vmware ESXi apresenta recursos de monitoramento das maquinas virtuais e do próprio host. Isso inclui monitoramento de recursos, desempenho em tempo real, eventos e alertas, integridade e segurança, além do registo detalhado de logs. Esses recursos ajudam actualmente os administradores a identificar problemas, optimizar o desempenho e garantir a disponibilidade contínua do ambiente virtualizado.

Os demais dispositivos como switches e AP's, não são monitorados activamente apenas no caso de anomalias. No caso da indisponibilidade de um AP, geralmente os administradores verificam as portas físicas do switch do modo a verificar se estão bem conectado ou não, caso esteja tudo em conformidade, verifica-se a nível de configurações se a porta encontra-se ligada e bem configurada.

No concernente a CCTV, é feita a verificação periódica das câmeras através do NVR (Network Video Recorder), é feita a verificação do espaço em disco, teste das gravações e reprodução de vídeos.

Em suma, actualmente o monitoramento é manual e para a maioria dos equipamentos e serviços é feito um monitoramento quando detecta-se uma anomalia e ou quando ocorre um problema.

3.4 Actividades realizadas no âmbito do estágio na ALTEL

O estágio foi em uma das empresas da Meridian32 que é neste caso a ALTEL, empresa esta responsável pelo parque tecnológico e zela pela infra-estrutura de rede da Meridian32.

O estágio teve duração de 6 meses, respeitando o horário laboral da ALTEL em que o horário de entrada era 8h com intervalo das 12:30 até as 14h e saída às 17:30.

A direcção da ALTEL optou por alocar o autor deste relatório a realizar trabalho de campo para melhor se enquadrar nas actividades diárias da empresa, onde desempenhava a função de Técnico de TI com auxílio do chefe do departamento de TI.

Durante esse perído foram realizados diversos trabalhos em diversas áreas onde a principal actividade foi desenvolvida na área de administração de sistemas.

As actividades principais que eram realizadas são: criação de máquinas virtuais, administração das máquinas, gestão dos acessos, instalação de serviços, monitoramento de sistemas, configuração de contas para estações de trabalho, criação de políticas de TI, configuração de impressoras, administração do microsoft365 entre outras tarefas.

3.4.1 Actividades em destaque

- **Migração do VMWARE da versão 5.5 para 6.7**

A infra-estrutura de servidores do Grupo Meridian32 era baseada na solução de virtualização VMWARE versão 5.5, que agora está obsoleta. Para solucionar isso, foi planejada uma migração da versão 5.5 para a versão 6.7. Aproveitando o repositório centralizado de máquinas virtuais, que é um armazenamento que fornece *datastores* para os servidores armazenarem os arquivos das máquinas virtuais, essa vantagem foi utilizada, incluindo a disponibilidade de servidores extras para realizar a migração do VMware.

Primeiramente, foi feita a instalação do VMware 6.7 nos servidores físicos extras. Em seguida, os *datastores* foram mapeados na nova versão e as máquinas virtuais foram transferidas para os servidores extras. O objetivo dessa migração para os servidores extras era garantir que os servidores anteriores, com a versão 5.5, ficassem livres para a instalação da nova versão do VMWARE posteriormente. A migração foi concluída com sucesso.

- **Migração dos sistemas operativos dos servidores virtuais**

Visto que o Windows server 2012R2 ficará sem suporte e será necessário que as empresas migrem para versões mais recentes, foi agendada uma tarefa de migração dos sistemas dos servidores da Meridian32.

Os servidores virtuais usavam o Windows Server 2012R2, a migração foi feita para Windows Server 2022.

Inicialmente foi feito uma *clean instalation*, que consiste em fazer uma instalação nova a partir da ISO do Windows Server, e foram instalados os serviços novamente sem utilização dos recursos antigos. Essa solução foi para quase todos servidores, exceptuando o Domain Control.

No caso do DC (Domain Control), foi instalado uma nova máquina na versão 2022, porém a posterior moveu-se os serviços do 2012 para 2022.

- **Projecto de montagem e configuração de sistemas de video conferência Booking System**

Durante o período de estágio profissional foi fornecido a fidelidade ímpar um sistema de vídeo conferência e 7 Sistemas da Clevertouch para agendamento de sala de reuniões.

Lista dos equipamentos fornecidos:

- 2 HP Presence Small room solution
- 3 Polystudio usb
- 1 Polystuido E70
- 7 Clevertouch Booking System

O autor desempenhou o papel principal como o técnico responsável do projecto, onde foi elaborado um plano para a execução das tarefas, o plano consistia em:

- Entrega do equipamento;
- Montagem e configuração dos sistemas de vídeo conferência;
- Montagem e configuração dos sistemas de agendamento de salas;

- Formação dos utilizadores; e
- Relatório das actividades desencadeadas no projecto.

Foi seguido o plano onde inicialmente fez-se a entrega do projecto, e seguindo a documentação dos equipamentos fez-se a instalação dos equipamentos. O projecto foi finalizado com sucesso.

4 CAPÍTULO IV – IMPLEMENTAÇÃO DA SOLUÇÃO

No presente capítulo é apresenta a solução e implementada a solução para o monitoramento da rede da Meridian32.

A solução para o problema descrito no trabalho é a implementação do sistema de monitoramento Zabbix. Com a implementação da seguinte ferramenta espera-se poder prever possíveis falhas e actuar de forma pró-activa do modo a evitar possíveis problemas que possam comprometer a disponibilidade da informação e dos serviços como também a segurança da rede corporativa da Meridian32.

A implementação do zabbix 6.0 foi feita com base na documentação do site oficial do zabbix *(http://zabbix.com)*.

Foi seguido um plano de implementação criado pelo autor que consistia em:

1. Escolher a versão ideal e o sistema operativo, neste caso foi escolhida a versão 6.0 LTS do Zabbix e Ubuntu Server 20.04
2. Criação da máquina virtual com recursos ideais para a instalação do ubuntu server que deverá hospedar a aplicação do zabbix
3. Instalação do zabbix 6.0 LTS no ubuntu server
4. Configuração básica do zabbix para monitoramentos e notificações
5. Monitoramento de Servidores virtuais

4.1 Instalação do Zabbix

Passo1: Criação da máquina virtual com nome Zabbix no Vmware ESXI 6.7 como ilustra a **figura 6.** Foi nesta máquina onde foi feita a instalação do sistema operativo ubuntu 20.04 que iria hospedar o zabbix 6.0 LTS. Foi seguido o processo de criação onde escolhe-se a ISO que a ser usada para a instalação do sistema operativo e o local onde será armazenada a informação do mesmo sistema.

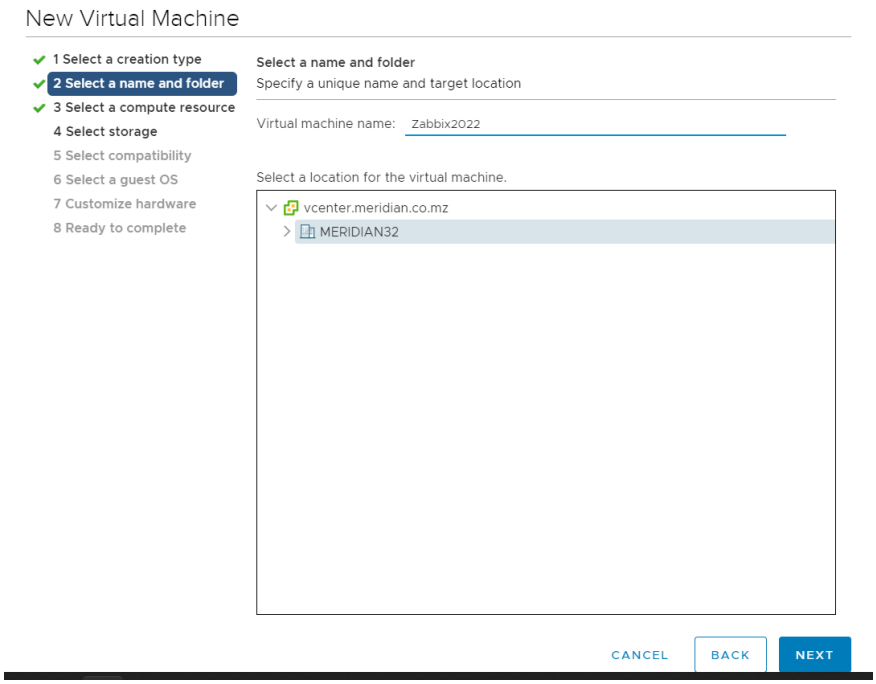

***Figura 7** - Criação de uma nova máquina virtual no esxi*

***Fonte:** Captura de tela feita pelo autor*

Passo 2: Instalação do **Zabix Server** na máquina virtual preparada no ESXI.

Após a preparação do ambiente para instalação do ubuntu 20.04, foi seguido o processo de instalação básico e durante o processo foi atribuído um IP a máquina virtual como ilustra a **figura 8.**

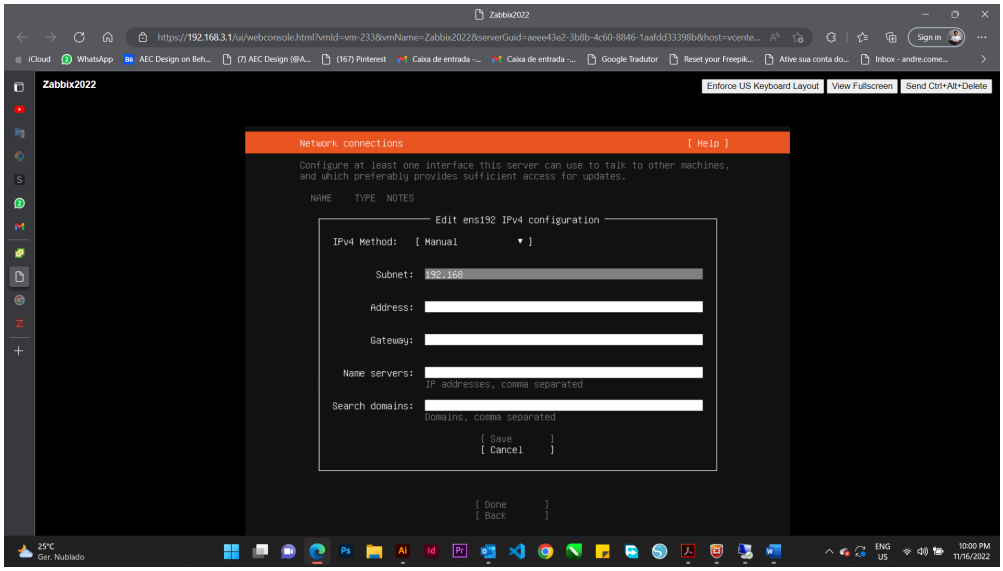

***Figura 8** - Configuração de IP durante o processo de instalação do ubuntu server 20.04*

***Fonte:** Captura de tela feita pelo autor*

Após a instalação do ubuntu server, foi habilatado o SSH para a conexão remota ao servidor via PUT e desta forma prosseguiu-se com a instalação do Zabbix via Linha de comando onde, fez-se o download do zabbix e a configuração da base de dados.

Passo 3: Finalização da instalação via interface web acedida através do IP atribuído a maquina virtual seguido de /zabbix como ilustra a **figura 9.**

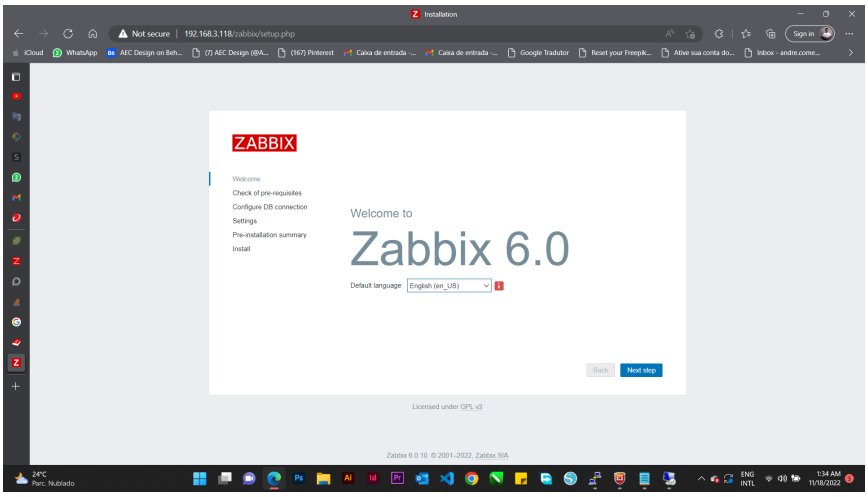

***Figura 9** - Interface web da finalização da instalação do Zabbix*

***Fonte:** Captura de tela feita pelo autor*

Passo 4: Foi nessa fase que foi feita a configuração do zabbix para que fosse possível monitorar diversos servidores e switchs, foi também nesta última fase onde foram configuradas as notificações por email e o serviço SNMP para monitoramento via SNMP. A **figura 10** ilustra a tela principal do Zabbix.

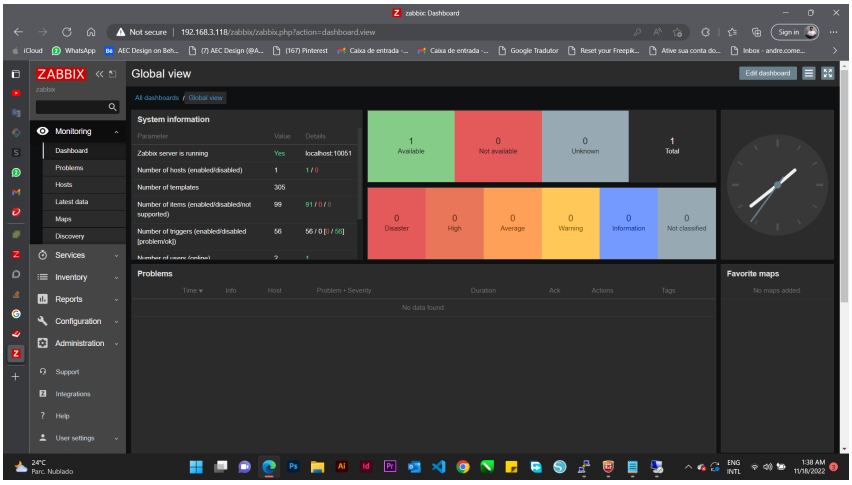

***Figura 10** - Tela principal do zabbix (Dashboard)*

***Fonte:** Captura de tela feita pelo autor*

Após a finalização da instalação e configuração, foram adicionados diversos dispositivos para serem monitorados pelo zabbix.

Para os servidores foi instalado o agente do Zabbix e implementado o template ***agent windows for zabbix.*** A instalação do agente foi feita máquina por máquina, onde durante a instalação colocou-se oI P do *Zabbix Server* e na configuração do *host* na aplicação *web* do zabbix foi adicionado o método de monitoramento por agente e inserido o IP da máquina virtual a ser monitorada.

Quanto aos outros dispositivos como switches, routers, warless control e access point's, foi usado o protocolo SNMPv2. Para tal foi necessário habilitar o SNMP no dispositivo e de seguida configurar a comunicadade e o IP do Zabbix Server.

Na configuração do host no Zabbix, foi inserido o template Cisco IOS SNMP para os switches, access point's e Wireless control. Para o NVR foi adicionado o template Generic SNMP e de seguida foram configurados a comunidade e os macros de acordo com as instruções da documentação do zabbix.

A **figura 11**, ilustra os hosts a serem monitorados pelo Zabbix, onde podemos ver a quantidade de problemas encontrados e o nível dos mesmos.

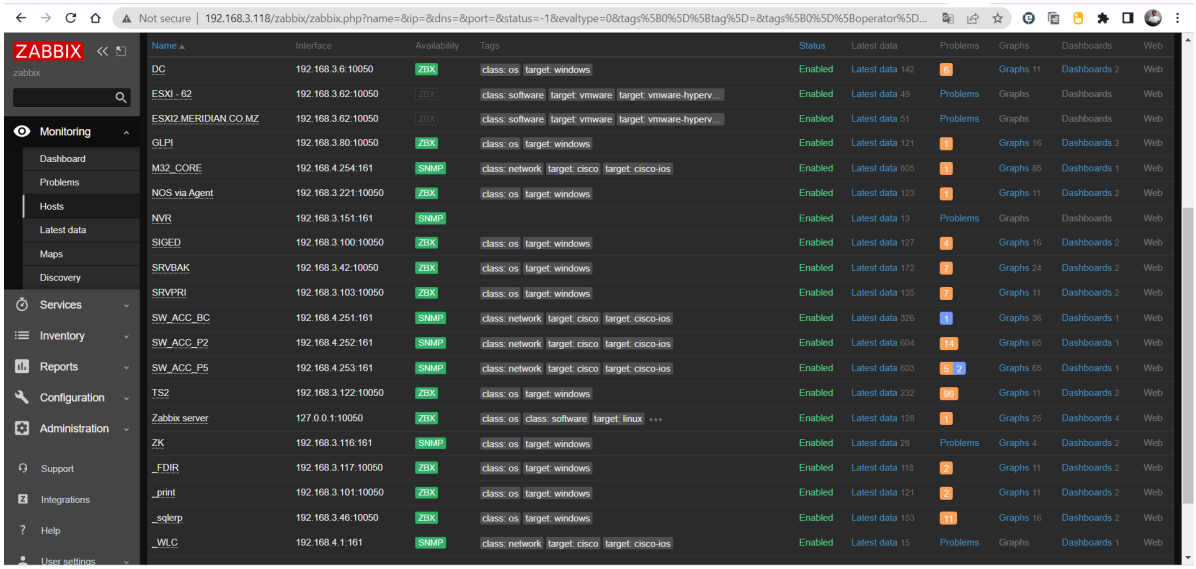

Figura 11 - Lista de hosts monitorados pelo Zabbix

Fonte: *Captura de tela feita pelo autor*

4.2 Monitoramento com Zabbix

A *dashboard* do Zabbix mostra os problemas ou informações detectadas pelos agentes ou pelo protocolo SNMP dependendo da situação como ilustra a **figura 12**. Do modo a alertar o administrador de redes para que ele possa agir de forma rápida evitando agravamento de certos problemas, foi configurado para que o Zabbix alertasse os problemas graves por email.

A **figura 12** ilustra log do email enviado pelo Zabbix para os administradores de rede, a **figura 13** ilustra o email recebido na caixa de emails.

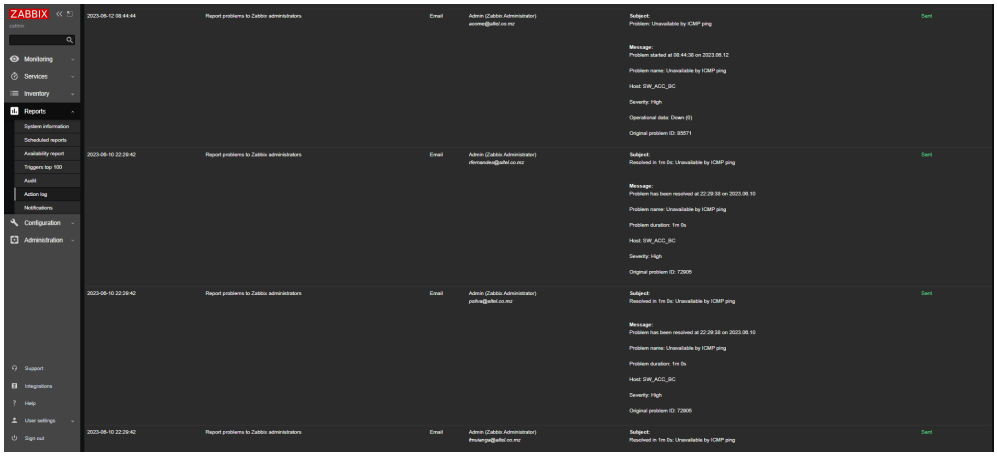

***Figura 12** - log do envio de alerta por email*

***Fonte:** Captura de tela feita pelo autor*

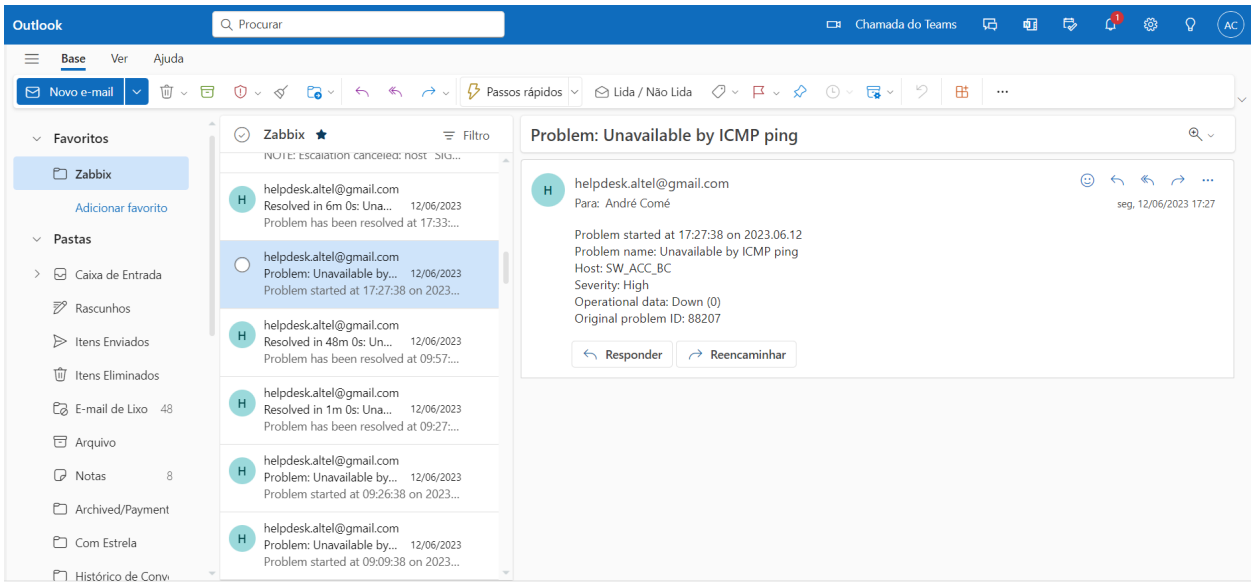

***Figura 13** - Email de alerta do Zabbix*

O monitoramento com o Zabbix proporciona uma série de vantagens e conclusões significativas para a gestão do ambiente de TI. Por meio da visibilidade em tempo real, é possível identificar problemas de forma rápida e ter uma compreensão completa da saúde do sistema. Com alertas pró-activos, é possível detectar eventos indesejados e agir antes que impactem o desempenho. Além disso, o Zabbix permite optimizar o desempenho, realizar o planejamento de capacidade com base em tendências e obter relatórios e análises detalhadas. Com essas conclusões, é possível tomar decisões estratégicas embasadas em dados confiáveis, melhorar a eficiência operacional e garantir a disponibilidade e o bom funcionamento dos sistemas.

5 CAPÍTULO V – CONCLUSÕES E RECOMENDAÇÕES

5.1 Conclusões

O presente relatorio procurou de forma geral arrolar sobre a importância do uso das ferramentas de monitoramento de redes de computadores. Nessa senda, objectivo central deste relatório como pesquisa aplicada é implementar sistema de monitoramento de rede de computadores Zabbix na Meridian32.

Em busca desse objectivo, um estudo de caso foi proposto na Meridian32, podendo assim mostrar resultados que comprovem a eficiência e eficácia de uma ferramenta de monitoramento neste caso concreto o Zabbix.

A implementação de sistema de monitoramento de rede de computadores contribui de modo geral, para facilitar as rotinas de trabalho do administrador de rede na Meridian32, o objectivo desta implementação foi alcançado, foi implementada a ferramenta Zabbix. A ferramenta pôde provar durante o período de estágio que é muito potente impactando assim na produtividade da Meridia32 como também das empresas por ela compostas. Assim podemos afirmar que a ferramenta apoia a disponibilidade dos serviços e a continuidade do negócio influenciando directamente no crescimento e na produção continua da Meridian32.

Com relação ao estágio, a ALTEL, representada pelos seus gestores, se mostrou aberta a ideias e críticas durante o período da execução das tarefas, isso contribuiu para o sucesso dos objectivos propostos.

Por fim, com o monitoramento da rede e dos serviços que nela operam, o administrador da rede tem completa gerência sobre a mesma, podendo identificar e prever falhas, gerando precisos relatórios de instabilidades para os gestores, bem como auxiliar em tomada de decisão em relação aos equipamentos e serviços ou ainda possibilidade de agregar novos serviços na rede.

5.2 Recomendações

Com base nas informações e resultados obtidos ao longo deste trabalho, algumas recomendações podem ser feitas a ALTEL concretamente por ser a empresa que faz a gestão da rede da Meridian32:

- Implementar uma política de monitoramento abrangente: É fundamental estabelecer uma política clara e abrangente de monitoramento de rede, que inclua todos os dispositivos e serviços críticos. Isso garantirá uma visão completa do ambiente de TI e permitirá a detecção precoce de problemas.

- Realizar revisões periódicas do sistema de monitoramento: É importante realizar revisões periódicas do sistema de monitoramento para avaliar sua eficácia, identificar possíveis melhorias e garantir que ele esteja alinhado com as necessidades em constante evolução da organização.

6 CAPÍTULO VI – REFERÊNCIAS BIBLIOGRÁFICAS

Alexander Clemm, P. (2007). Network Management Fundamental. United States of America: Cisco Press. Obtido em 12 de 4 de 2023, de https://cs.petrsu.ru/~vadim/books/Network%20Management%20Fundamentals.pdf

Andreoli, Y. (2016). Análise comprativa entre ferramentas para gerenciamento e monitoramento de redes. Obtido em 5 de Julho de 2023, de https://repositorio.utfpr.edu.br/jspui/bitstream/1/15568/1/PB_COADS_2016_2_05.pdf

Bezerra, T. L. (15 de Abril de 2015). *SNMP II: Estudo de Caso – Preparação CACTI*. Obtido em 5 de Julho de 2023, de Teleco: https://www.teleco.com.br/tutoriais/tutorialsnmpred2/pagina_2.asp

Cacti. (s.d.). Obtido em 5 de Julho de 2023, de https://www.cacti.net/info/cacti

Cadorin, D. B. (2003). Ferramenta para monitoramento de Redes IP com Serviços. Florianópolis. Obtido em 3 de 3 de 2023, de https://repositorio.ufsc.br/xmlui/bitstream/handle/123456789/86381/198119.pdf?sequence=1

Core, N. (s.d.). *Nagios Core Documentation*. Obtido em 6 de Julho de 2023, de https://assets.nagios.com/downloads/nagioscore/docs/nagioscore/3/en/toc.html

Durieux, A. F. (2012). Monitoramento de servidores com scripts. Florianópolis.

Eler, E. d. (19 de Outubro de 2015). *Teleco*. Obtido em 15 de Maio de 2023, de Modelo TMN: Aplicação ao Gerenciamento de Redes de Telecomunicações: https://www.teleco.com.br/tutoriais/tutorialmodelotmn/pagina_2.asp

Forouzan, B. A. (2007). Data Communications and Networking. *4th*. New York: McGraw-Hill. Obtido em 5 de 3 de 2023, de file:///C:/Users/AEC/Downloads/EP/Data%20Communications%20and%20Networking%20By%20Behrouz%20A.Forouzan.pdf

King, N. (30 de Janeiro de 2023). *Melhores ferramentas de monitoramento de rede para 2023*. Obtido em 05 de Maio de 2023, de Network King: https://network-king.net/pt-pt/ferramentas-de-monitoramento-de-rede/

Nagios. (s.d.). *Nagios*. Obtido em 5 de Julho de 2023, de https://www.nagios.org/about/

Shokhin, A. (Maio de 2015). Network monitoring. Obtido em 15 de 3 de 2023, de https://core.ac.uk/download/pdf/38124402.pdf

Tanenbuam, A. S., & Wetherall, D. J. (2011). Computer Networks. (5th). (P. Education, Ed.) Obtido em 12 de 3 de 2023, de https://csc-knu.github.io/sys-prog/books/Andrew%20S.%20Tanenbaum%20-%20Computer%20Networks.pdf

Vachon, B., & Graziani, R. (2008). Accessing the WAN, CCNA Exploration Companion Guide. (C. Press, Ed.) United States of America. Obtido de https://ptgmedia.pearsoncmg.com/images/9781587132056/samplepages/1587132052.pdf

Yano, I. H. (Dezembro de 2010). Gerenciamento de Redes de Computadores utilizando CACTI. (1. Edição, Trad.) Campinas, SP. Obtido em 5 de Julho de 2023

Zabbix LLC. (11 de Junho de 2021). *Zabbix Manual.* Obtido em 6 de Julho de 2023, de https://www.zabbix.com/documentation/6.0/downloads/Zabbix_Documentation_6.0.en.pdf