UNIVERSIDADE FEDERAL DE SANTA CATARINA
Departamento de Informática e Estatística - INE
Sistemas de Informação
Administração e Gerência de Redes de Computadores
Florianópolis-SC, Brasil
Abril de 2025

Análise e Monitoramento de uma Rede Computacional Utilizando Zabbix e Wireshark

Abmael Batista da Silva[1]

Resumo

Este trabalho visa o monitoramento de uma rede domiciliar, composta por vários dispositivos usando a ferramenta Zabbix. A ideia é utilizar a ferramenta para verificar algumas características principais da rede, como desempenho e estabilidade. Além disso, neste trabalho serão aplicados diversos conceitos de redes, que serão exercitados durante a configuração das ferramentas e do ambiente. O trabalho também aborda o acordo do nível de serviço (SLA) para comparar a qualidade contratada com a prestada. Por último, será feito uso também da ferramenta Wireshark para algumas medições de pacotes enviados pela Rede.

Palavras-chave: Monitoramento; Zabbix; Redes; Wireshark.

[1] Graduando do Curso Sistemas de Informação - UFSC, Disciplina Informática e Sociedade.

SUMÁRIO

1. DESCRIÇÃO DA CONFIGURAÇÃO DOS RECURSOS E DA REDE

A rede é composta por três máquinas: um notebook, que funciona como host principal onde será instalado o Zabbix Server; Uma máquina virtual que atuará como agente monitorada; e um smartphone que será o host não monitorado. Todos os dispositivos estão conectados através de uma rede Wi-fi. A rede é doméstica com alguns hosts criados exclusivamente para fins experimentais do trabalho. Além dos três dispositivos mencionados, há um modem da marca Arris, responsável por fornecer acesso à internet para todos os dispositivos da rede, via infraestrutura da provedora.

1.1. CONFIGURAÇÕES E CARACTERÍSTICAS DOS HOSTS

Tabela 1. Configuração dos dispositivos da Rede Gerenciada

Hostname	Tipo	SO	Endereço IP	Tipo de Conexão	Modelo	RAM	Processador
Modem/Roteador	Gateway	Firmware embutido	192.168.0.1	Access Point (Wi-Fi)	Arris TG1692A	-	-
Notebook	Server/Gerente	Fedora Linux 41	192.168.0.44 (DHCP)	Wi-Fi	Dell Latitude 4000	16 GB	Intel Core i5 7gen (Quad-Core 3 GHz)
CentOS7-VM	Agente	CentOS7	192.168.0.83 (DHCP) 10.0.2.15 (NAT)	Wi-Fi	-	-	-
Smartphone	Agente (não monitorado)	Android 14	192.168.0.4 (DHCP)	Wi-Fi	Samsung Galaxy S21fe	8 GB	Exynos 2100 (Octa-Core 2.5 GHz)

Fonte: Elaborado pelo autor

2. TOPOLOGIA DA REDE MONITORADA

A topologia está representada graficamente na imagem abaixo. Nela, é possível identificar:

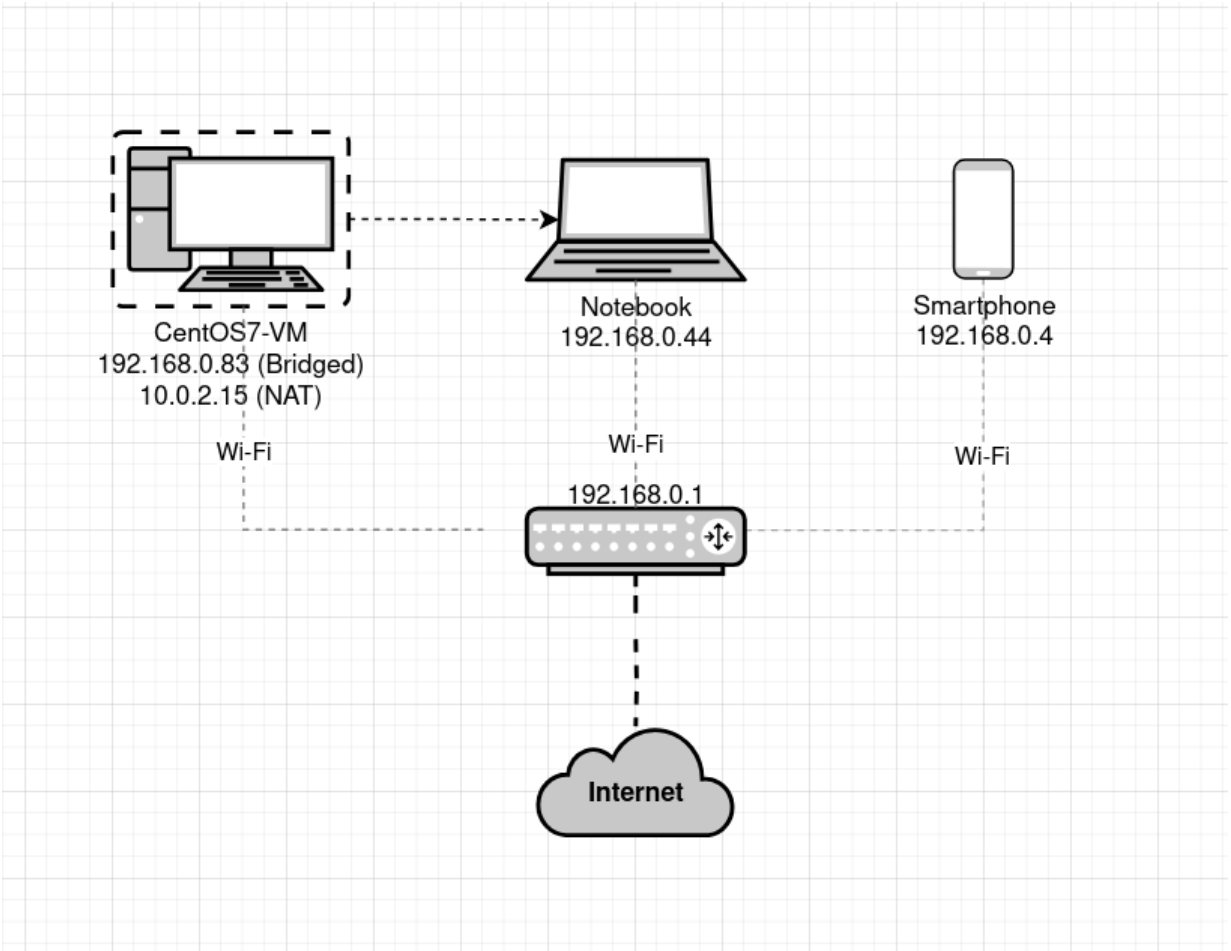
- O **Notebook**, que atuará como processo gerente e hospeda o **Zabbix Server**;
- A **máquina virtual CentOS7-VM**, criada por meio da ferramenta **Vagrant** em conjunto com o **VirtualBox**. Ela possui uma interface **NAT**, utilizada para conexão via

SSH e acesso à internet, e outra interface em modo **Bridged**, que permite a comunicação com o servidor Zabbix e será monitorada como um agente da rede;

- O **Smartphone**, que atuará como um dispositivo não monitorado pelo **Zabbix**;
- E o **Roteador** Arris, posicionado ao centro da topologia, fornecendo acesso à internet para todos os dispositivos.

Essa topologia foi projetada para simular um ambiente gerenciado com diferentes papeis de dispositivos, permitindo observar o funcionamento do monitoramento via Zabbix em um cenário realista.

Figura 1. Topologia da rede utilizada no trabalho.



Fonte: Elaborado pelo autor.

3. FERRAMENTAS UTILIZADAS PARA GERÊNCIA

A ferramenta principal utilizada para a gerência da rede é o **Zabbix na sua versão 7.2**, uma solução de nível enterprise, de código aberto, com suporte à monitoração distribuída. O Zabbix permite monitorar diversos parâmetros da rede, servidores e a saúde dos serviços. Conta com um mecanismo flexível de notificação que possibilita configurar alertas por e-mail

para praticamente qualquer evento, permitindo uma resposta rápida a problemas no ambiente. Além disso, oferece excelentes recursos de relatórios e visualização de dados armazenados, o que o torna uma ferramenta ideal para atividades de gerência e monitoramento de redes.

Além do Zabbix, também foi utilizada a ferramenta **Wireshark** para realizar análises de tráfego da rede, identificação de pacotes e diagnóstico de problemas de comunicação entre os dispositivos monitorados. O Wireshark é uma ferramenta essencial para a inspeção detalhada de protocolos de rede em tempo real.

4. INSTALAÇÃO E TESTES INICIAIS DO ZABBIX

4.1 INSTALANDO O ZABBIX SERVER, DATABASE E FRONTEND COM DOCKER.

O Zabbix Server é o backend da aplicação, responsável por todos os métodos e operações de monitoramento. O **Zabbix Database** é o banco de dados do servidor, onde ficarão armazenadas as informações de gerência e dos agentes. Já o Zabbix Frontend é responsável pela interface web que permite as interações do usuário com o sistema de monitoramento. A instalação de todos esses componentes será feita através do **Docker** dentro da máquina **Notebook**, colocando cada parte do sistema como um Container. O passo a passo oficial da instalação via containers está disponivel na documentação oficial do Zabbix: https://www.zabbix.com/documentation/7.0/en/manual/installation/containers

Pré-requisitos e configuração do ambiente

Como pré-requisito, é preciso ter instalado o Docker e Docker Compose instalados na máquina. Para instalar no Fedora Linux ou distribuições baseadas em RedHat utilizar o comando:

```
sudo dnf install docker docker-compose
```

Em seguida, dentro do repositório que será utilizado para a manter os arquivos do sistema, baixar o repositório oficial do Zabbix com os arquivos **docker-compose**:

```
git clone https://github.com/zabbix/zabbix-docker.git
```

Subindo os containers com Docker Compose

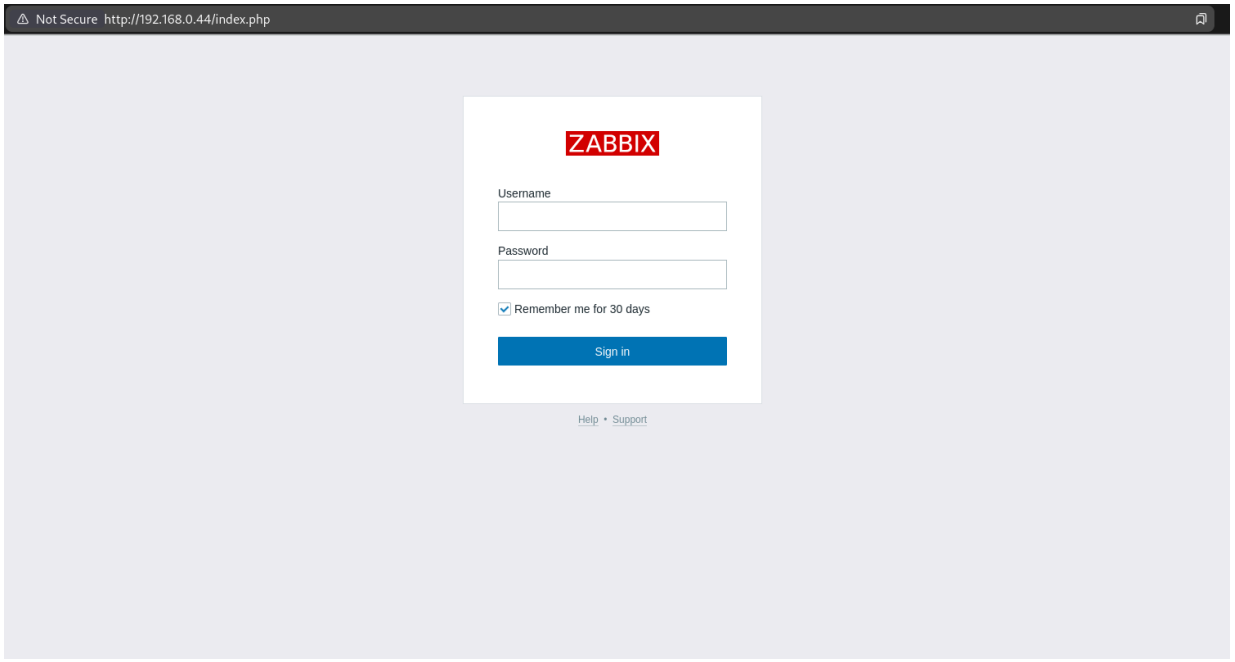
No meu caso, optei pela versão com alpine linux e versão mais recente do mysql. O comando abaixo sobe, através do docker compose, os containers com o zabbix-server, zabbix-database e zabbix-web (frontend).

```
sudo docker compose -f ./docker-compose_v3_alpine_mysql_latest.yaml up -d
```

Acessando a interface web do Zabbix:

O zabbix-frontend poderá ser acessado pela url: http://192.168.0.44/zabbix.

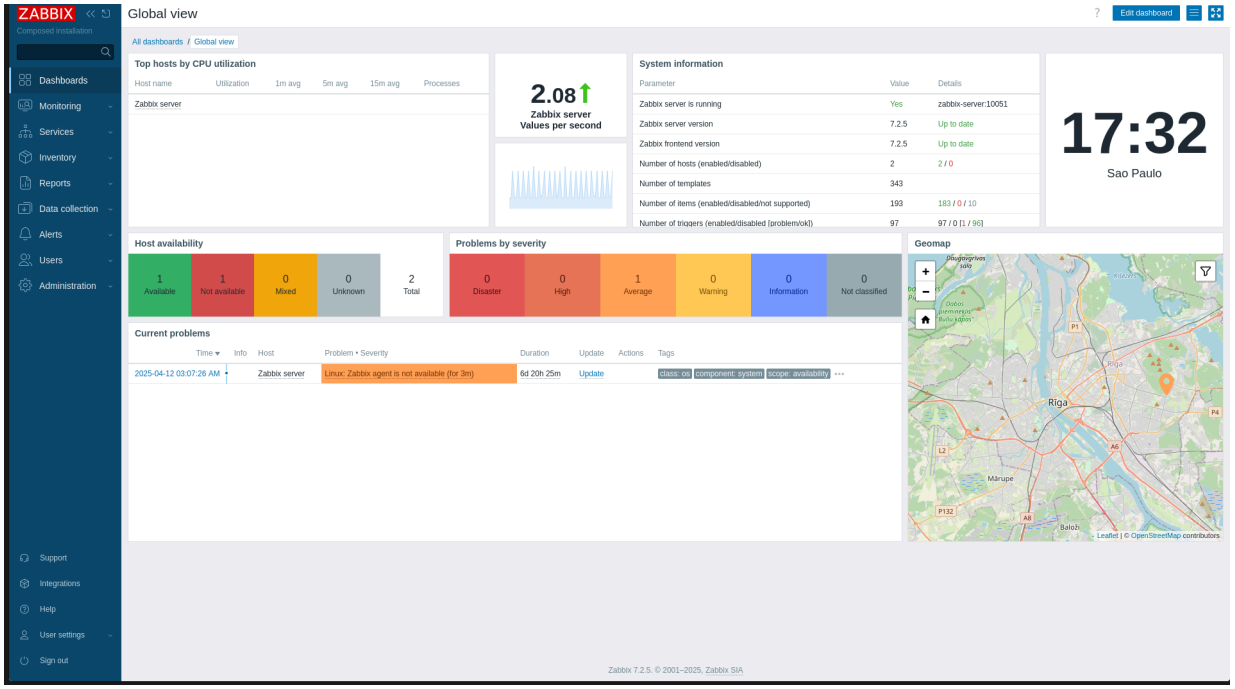
Figura 2. Tela de Login do Zabbix Frontend.



Fonte: Elaborado pelo autor

O login por padrão é feito com o usuário **Admin** e senha **zabbix**. Ao acessar o sistema é possível visualizar o dashboard inicial com algumas informações configuradas por default.

Figura 3. Tela inicial do Zabbix Frontend.



Fonte: Elaborado pelo autor

4.2. INSTALAÇÃO DO ZABBIX AGENT

O Zabbix Agent é o serviço responsável por permitir coletar informações e monitorar os recursos da máquina onde o agente está instalado. Para o nosso teste, ele será instalado na máquina CentOS7-VM, conforme o passo a passo.

Adicionando o repositório oficial do Zabbix no CentOS 7

Executar o comando abaixo para adicionar o repositório da versão 6.4 do Zabbix

```
rpm -Uvh https://repo.zabbix.com/zabbix/6.4/rhel/7/x86_64/zabbix-release-6.4-1.el7.noarch.rpm
```

Em seguida, atualize os pacotes do sistema:

```
yum clean all
```

Instalando o Zabbix Agent

Com o repositório configurado, instalar utilizando o comando abaixo:

```
yum install -y zabbix-agent
```

Editar o arquivo de configuração do Zabbix Agent

O arquivo deve ser configurado para estabelecer a comunicação com o server

```
vi /etc/zabbix/zabbix_agentd.conf
```

Alterar ou adicione as linhas abaixo:

```
# Alterar para o IP do servidor
Server=192.168.0.44

# Colocar um nome para o host. Este será o nome cadastrado no server.
Hostname=CentOS7-VM

# Indicar o IP do servidor ativo que por padrão, é o mesmo acima.
ServerActive=192.168.0.44
```

Liberando a porta no firewall

É necessário permitir a comunicação do agente com o Servidor através da porta 10050:

```
firewall-cmd --permanent --add-port=10050/tcp
firewall-cmd --reload
```

Habilitando e iniciando o serviço do Zabbix Agent

```
systemctl start zabbix-agent
systemctl enable zabbix-agent
```

Criando novo Host no Zabbix Server

Com o zabbix-agent rodando, voltamos na interface Web do Zabbix Server para inclusão de um novo host:

1. Vá para as configuraçẽos → Hosts
2. Clique em "Create host"
3. Preencher as informações conforme abaixo:
    a. **Host name:** CentOS7-VM (deve ser igual ao cadastrado no Agent)
    b. **Groups:** Adicione um grupo apropriado (e.g., "Linux servers")
    c. **Interfaces:** Adicionar a interface IP da CentOS VM 192.168.0.83
    d. **Templates:** É possível incluir um template, com algumas configurações e indicadores prontos para uso. Para o nosso host, utilizamos o **Linux by Zabbix agent.**
4. Clicar em "**Add**" para salvar.

5. MEDIÇÕES INICIAIS NO ZABBIX

Após configurar o host, é possível realizar alguns testes iniciais para verificar se a monitoração está funcionando.

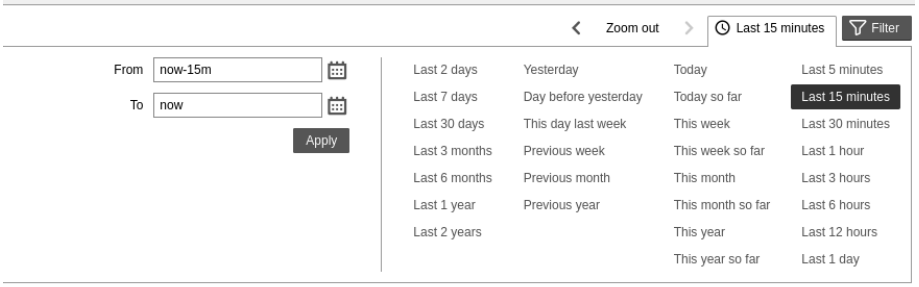
1. Acesse o menu **Monitoring → Hosts**.
2. Verifique se o host aparece como **"Available"** (ícone verde).
3. Selecione o host e vá até a aba **Graphs** para visualizar gráficos prontos.

Figura 4. Tela com as informações dos hosts cadastrados.

Fonte: Elaborado pelo autor.

Para um teste inicial, vamos analisar a quantidade de Bits que estão passando pelas interfaces de rede Wi-Fi do host. Na Figura 6 e 7, é possível visualizar o gráfico de bits enviados e bits recebidos dentro dos últimos 15 minutos conforme os filtros na Figura 5:

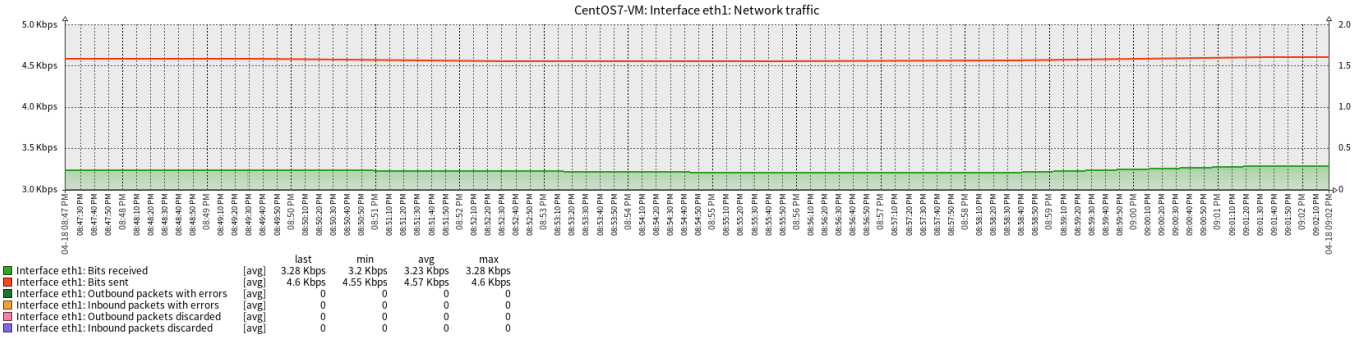
Figura 5. Filtro de período utilizado nos testes iniciais.



Fonte: Elaborado pelo autor

A interface **eth1** (DHCP) é utilizada para a conexão com o servidor mas não possui acesso à internet. Portanto, seu gráfico mostra baixa ou nenhuma oscilação:

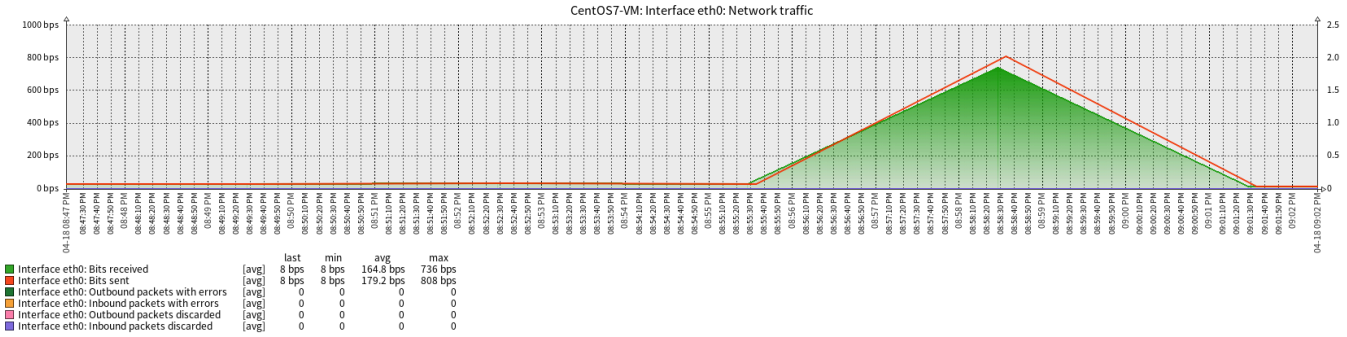
Figura 6. Gráfico de bits enviados e recebidos na interface eth1.



Fonte: Elaborado pelo autor

A interface **eth0** é a interface NAT do sistema, com IP 10.0.2.15, responsável por prover o acesso à internet. No gráfico abaixo, é possível ver uma oscilação nos bits enviados e recebidos, após um ping no DNS da Google (8.8.8.8):

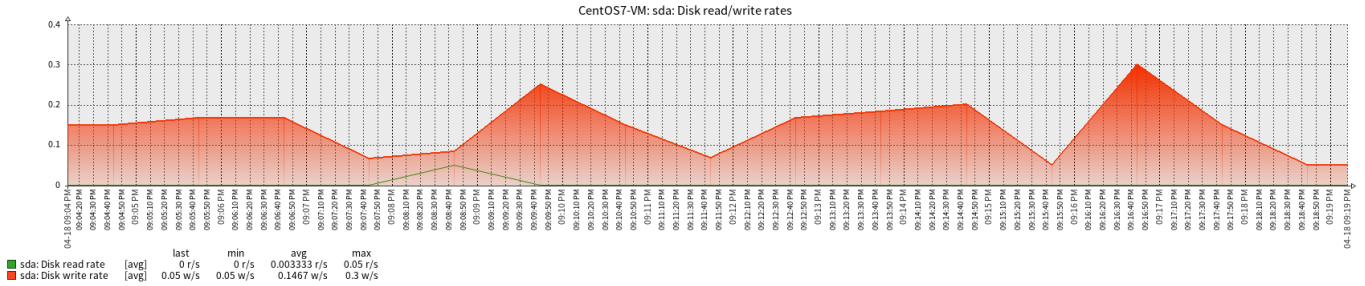
Figura 7. Gráfico de bits enviados e recebidos na interface eth0



Fonte: Elaborado pelo autor

Além disso, como o host foi configurado com o template padrão do Zabbix, também é possível visualizar outros dados como **leituras e escritas em disco**, **uso de CPU**, **uso de memória**, entre outros.

Figura 8. Leitura e escrita no disco da VM.



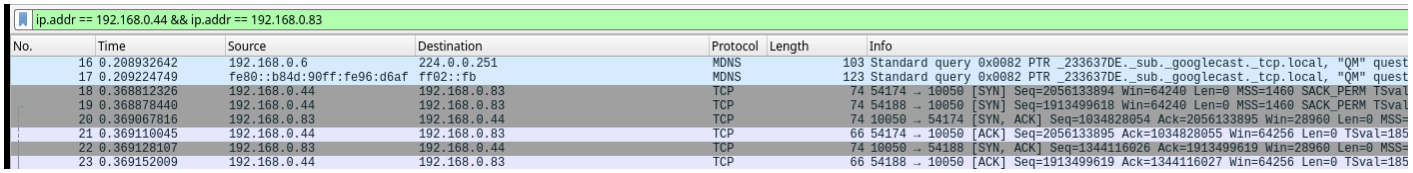
Fonte: Elaborado pelo autor

6. MEDIÇÕES INICIAIS NO WIRESHARK

Durante a execução inicial do monitoramento com Zabbix, foi realizada uma captura de pacotes utilizando o Wireshark, focando na comunicação entre o notebook (servidor Zabbix - IP 192.168.0.44) e a máquina virtual CentOS7 (agente Zabbix - IP 192.168.0.83).

Os pacotes capturados mostraram o estabelecimento da conexão via protocolo TCP, através das portas padrão 10050 (para requisições passivas do servidor ao agente) e 10051 (para verificações ativas do agente ao servidor).

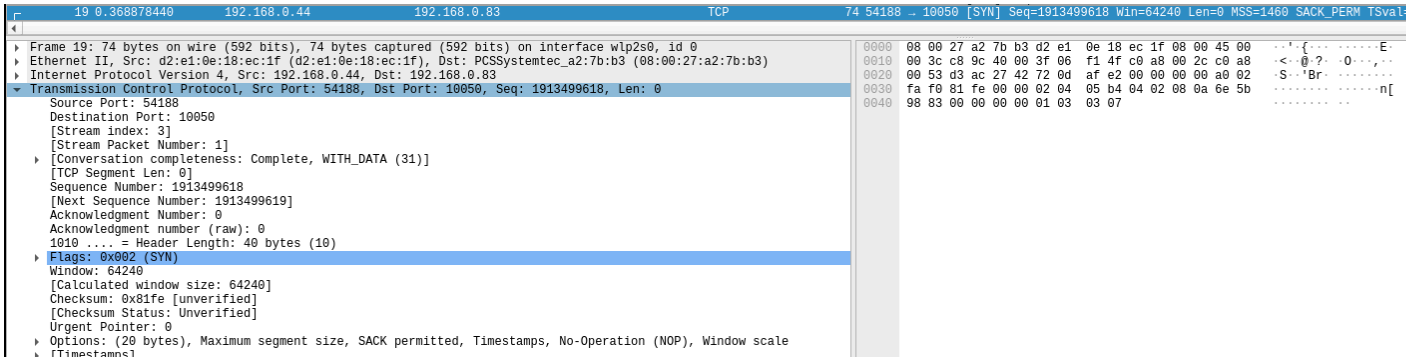
Figura 9. Visão geral da conexão TCP entre o Server e o Agent.



Fonte: Elaborado pelo autor.

Na Figura 10 abaixo, é possível observar com detalhes a requisição feita do gerente (192.168.0.44) para o Agent (198.168.0.83) como parte da verificação do protocolo:

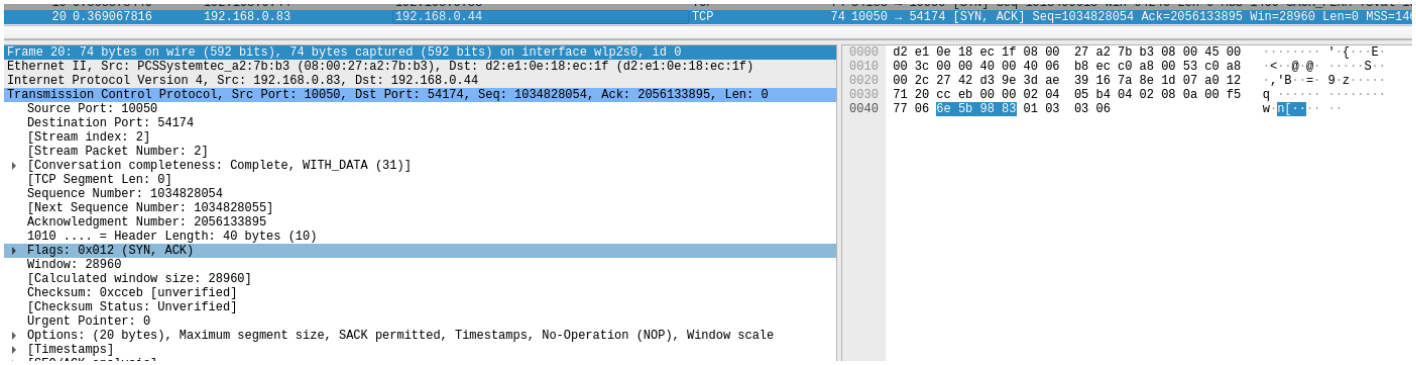
Figura 10. Cabeçalho com a requisição SYN do TCP



Fonte: Elaborado pelo autor.

Ja na Figura 11, podemos ver a resposta do Agent para o Gerente com os dados necessários para a sincronização entre ambos:

Figura 11. Resposta SYN e ACK para sincronização entre agent e gerente.



Fonte: Elaborado pelo autor.

7. QUESTIONÁRIO DE SATISFAÇÃO DOS USUÁRIOS

O seguinte questionário foi aplicado aos usuários da rede com o objetivo de avaliar a percepção aos serviços prestados:

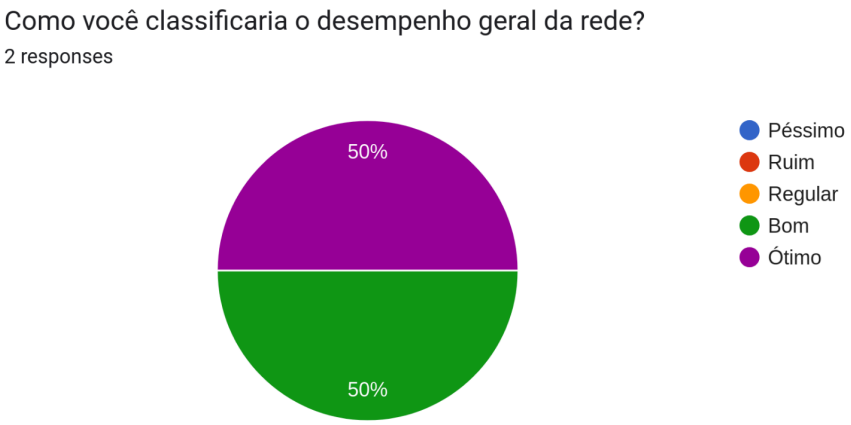
1. Como você classificaria o desempenho geral da rede?
2. O quão estável é a rede? E a disponibilidade dos serviços?
3. Classifique em relação ao tempo gasto para que o suporte técnico resolva eventuais problemas.
4. Como é a qualidade dos serviços fornecidos pelo suporte técnico?
5. Como é a qualidade do acesso à rede externa (Internet)?
6. Como é a qualidade dos serviços prestados?
7. Como é a qualidade da segurança da rede?

A pesquisa teve um total de 2 pessoas participantes, que utilizam a rede. Os resultados são observados em seguida.

7.1. Como você classifica o desempenho geral da rede?

A primeira pergunta buscou uma avaliação abrangente do desempenho da rede. Conforme as respostas obtidas, é possível ver a satisfação geral da rede, com baixa margem para melhorias.

Figura 12. Gráfico com os resultados da pergunta 1.

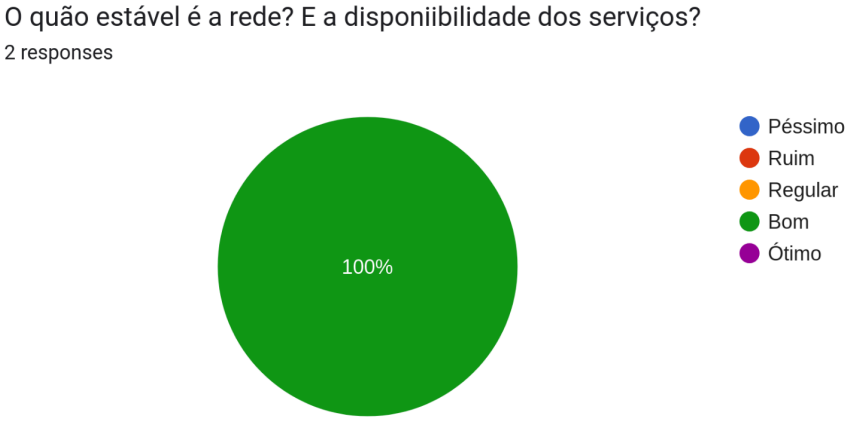


Fonte: Elaborado pelo autor.

7.2. O quão estável é a rede? E a disponibilidade dos serviços?

Para a segunda pergunta, que visa avaliar a estabilidade e disponibilidade da rede, a maioria dos usuários considera bom, indicando uma satisfação ok, mas com um pouco de margem para melhorias.

Figura 13. Gráfico com os resultados para a pergunta 2.

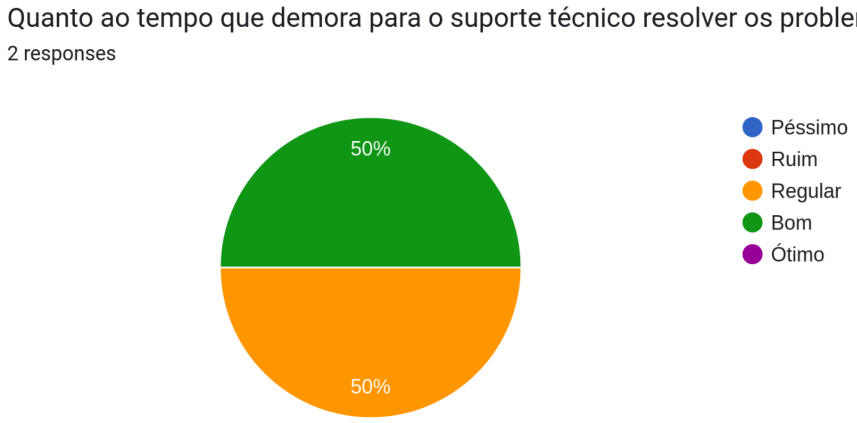


Fonte: Elaborado pelo autor.

7.3. Classifique em relação ao tempo gasto para que o suporte técnico resolver os problemas.

Para a terceira pergunta, que visa avaliar o tempo para suporte técnico, os usuários avaliam como bom ou regular. Isso indica que está dentro do esperado, mas espera-se um pouco mais de rapidez pelo time de suporte.

Figura 14. Gráfico com os resultados para a pergunta 3.

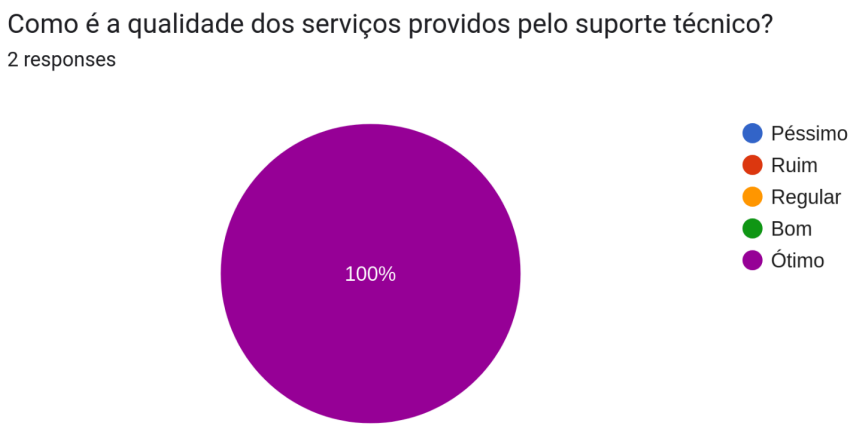


Fonte: Elaborado pelo autor.

7.4. Como é a qualidade dos serviços fornecidos pelo suporte técnico.

Para a quarta pergunta, que visa avaliar a qualidade dos serviços do suporte, ambos os usuários avaliam como ótimo. Isso indica que a qualidade está ótima e não é necessário nenhuma melhoria

Figura 15. Gráfico com os resultados para a pergunta 4.

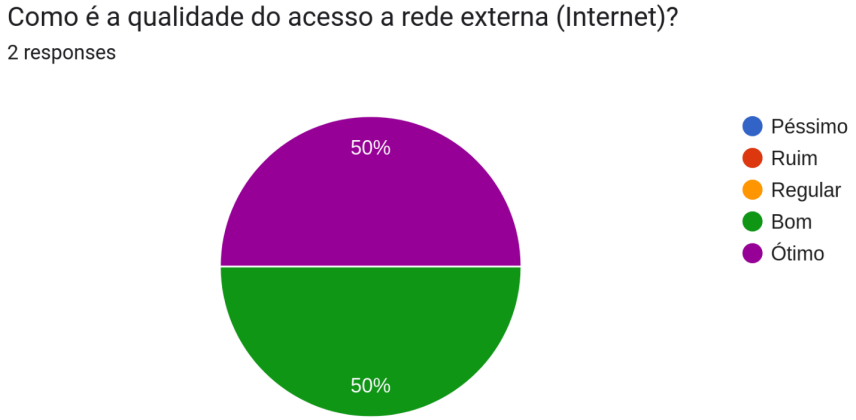


Fonte: Elaborado pelo autor.

7.5. Como é a qualidade do acesso à rede externa (Internet).

Para a quinta pergunta, que visa avaliar a qualidade do acesso a internet, os usuários avaliam como ótimo ou bom. Indica que o acesso está satisfatório, com baixa necessidade de melhoria.

Figura 16. Gráfico com os resultados para a pergunta 5.

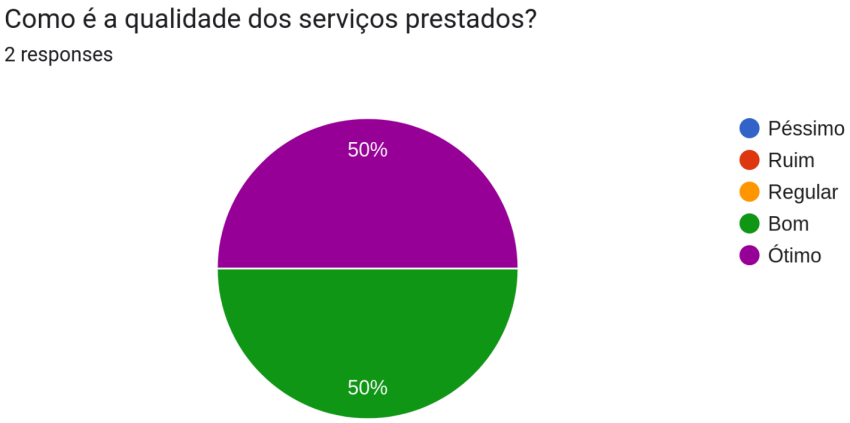


Fonte: Elaborado pelo autor.

7.6. Como é a qualidade dos serviços prestados.

Para a sexta pergunta, que visa avaliar a qualidade prestada no geral para a rede, os usuário avaliam como ótimo ou bom. Indica que a qualidade está satisfatória, mas que pode haver pequenas melhorias para satisfação total.

Figura 17. Gráfico com os resultados para a pergunta 6.

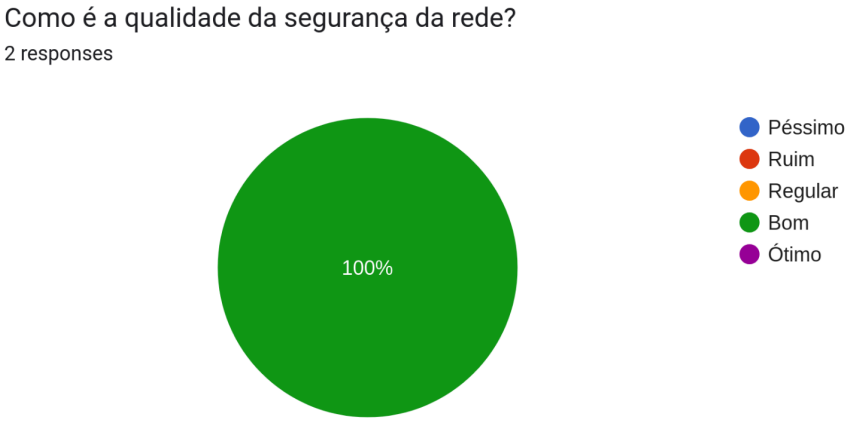


Fonte: Elaborado pelo autor.

7.7. Como é a qualidade da segurança da rede?

Para a sétima pergunta, que visa avaliar a segurança geral para a rede, ambos os usuários avaliam como bom. Indica que a segurança esta boa, mas que pode ter uma melhora.

Figura 18. Gráfico com os resultados para a pergunta 7.



Fonte: Elaborado pelo autor.

8. ACORDO DE NÍVEL DE SERVIÇO

8.1 CLÁUSULAS DO SLA - DESCRIÇÃO GERAL

Tabela 3. Clausulas do SLA.

Nº	Cláusula	Descrição
1	Objetivo do SLA	Estabelecer parâmetros mínimos de desempenho, suporte e disponibilidade.
2	Escopo	Aplica-se à rede local composta por notebook, VMs e roteador doméstico.
3	Disponibilidade da rede	Garantia de 95% de disponibilidade mensal da rede.
4	Tempo de resposta do suporte	Tempo máximo de 30 minutos para resposta a incidentes críticos.
5	Serviços monitorados	Acesso à internet, comunicação entre hosts, serviços em VMs.
6	Penalidades	Multas simbólicas ou aviso formal em caso de descumprimento de SLA.
7	Requisitos de Segurança	Criptografia no tráfego interno e bloqueio de portas desnecessárias.
8	Monitoramento e métricas	Realizado por Zabbix, com relatórios semanais e alertas automáticos.
9	Período de vigência	SLA válido por 6 meses a partir da data de implementação.

Fonte: Elaborado pelo autor.

8.2 SLA COMPLETO - TEXTO FORMAL

Contrato de Acordo de Nível de Serviço (SLA)

Entre as partes:

Prestador: Responsável técnico pela gestão e monitoramento da rede descrita neste documento.

Usuários: Todos os indivíduos e sistemas que fazem uso da rede computacional monitorada.

CLÁUSULA 1 - OBJETIVO

Este Acordo de Nível de serviço tem como objetivo definir os compromissos, garantias e responsabilidades relativos à prestação dos serviços da rede, com base nos recursos disponíveis, desempenho esperado e nível de suporte técnico oferecido. Este documento visa assegurar a transparência entre o prestador e os usuários da rede.

CLÁUSULA 2 – ESCOPO

O presente SLA aplica-se à infraestrutura de rede local composta por:

- Um notebook (servidor principal, com Zabbix instalado);
- Uma máquina virtual (clientes monitorados);
- Um smartphone (host não monitorado);
- Um roteador doméstico (gateway de acesso à internet).

Estes dispositivos fazem parte de uma rede residencial com fins educacionais e de teste.

CLÁUSULA 3 – DISPONIBILIDADE DA REDE

Fica estabelecido que a rede deverá manter um índice mínimo de 95% de disponibilidade mensal, exceto em casos de:

- Falhas de energia elétrica;
- Manutenção programada;
- Fatores externos que impeçam a operação da infraestrutura.

CLÁUSULA 4 – TEMPO DE RESPOSTA DO SUPORTE TÉCNICO

Ocorrendo incidentes ou falhas, o tempo máximo de resposta do responsável técnico deverá ser de:

- Até 30 minutos para incidentes críticos (ex: perda total de conectividade);
- Até 2 horas para incidentes de médio impacto;
- Até 6 horas para solicitações de baixa prioridade ou informativas.

CLÁUSULA 5 – SERVIÇOS MONITORADOS

Estão incluídos neste SLA os seguintes serviços:

1. Monitoramento de disponibilidade e desempenho dos hosts monitorados (VMs);
2. Análise de tráfego de rede (bits in/out);
3. Verificação de leitura/escrita em disco;

4. Acesso à internet e conectividade entre dispositivos internos.

CLÁUSULA 6 – PENALIDADES E NÃO CONFORMIDADES

Em caso de descumprimento recorrente deste SLA, o prestador poderá ser advertido formalmente, considerando que este é um ambiente de testes. Este documento não implica em obrigações financeiras, mas sim em compromissos acadêmicos e operacionais.

CLÁUSULA 7 – SEGURANÇA DA REDE

O ambiente deverá obedecer aos seguintes requisitos de segurança:

- Acesso restrito via autenticação local (Basic Auth & SSH);
- Monitoramento contínuo de portas e serviços via Zabbix;
- Utilização de firewall ativo nas máquinas monitoradas;
- Uso de NAT para isolamento da rede local.

CLÁUSULA 8 – MONITORAMENTO E MÉTRICAS

A verificação dos parâmetros estabelecidos será feita através da ferramenta Zabbix, instalada no host principal. Serão gerados relatórios semanais com métricas de desempenho, alertas e gráficos. O histórico de eventos será utilizado para avaliação de conformidade com este SLA.

CLÁUSULA 9 – VIGÊNCIA DO ACORDO

O presente acordo entra em vigor na data de implantação do monitoramento e terá validade de 6 (seis) meses, podendo ser revisado ou renovado conforme necessidade.

Florianópolis, 20 de Abril de 2025.

9. ACORDO DE NÍVEL DE SERVIÇO EM UML

O diagrama de classes apresentado modela um sistema de gerenciamento de SLA (Service Level Agreement), ou Acordo de Nível de Serviço, destacando as principais entidades envolvidas e suas inter-relações.

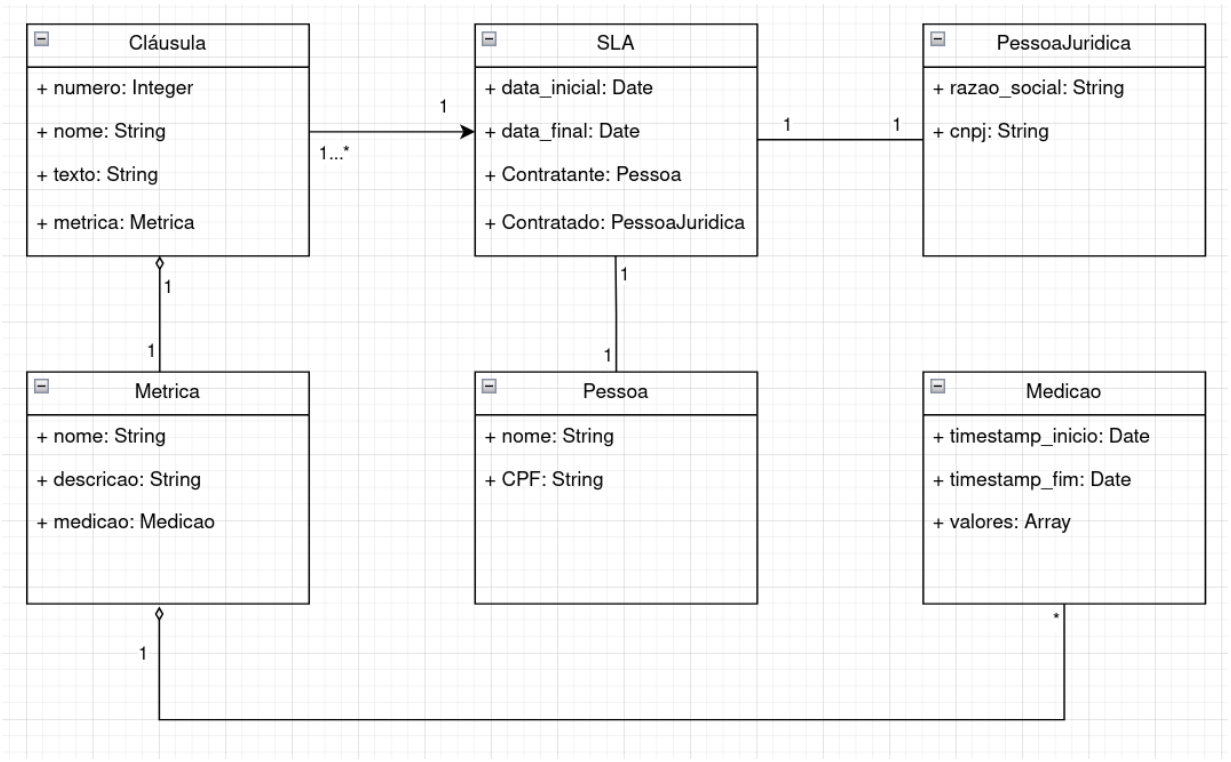
O SLA é representado por uma classe que contém as datas de início e fim do contrato, além das referências ao contratante, uma pessoa física (Pessoa), e ao contratado, uma pessoa jurídica (PessoaJuridica).

Cada SLA está associado a uma ou mais cláusulas (Cláusula), que definem as condições específicas do acordo. As cláusulas possuem atributos como número, nome e texto

descritivo, e estão ligadas diretamente a uma métrica (Metrica), a qual determina como aquela cláusula será medida e avaliada.

A métrica, por sua vez, está associada a uma medição (Medicao), que registra os dados reais obtidos durante o período de vigência da cláusula, incluindo informações como timestamps de início e fim e um conjunto de valores observados. Essa estrutura permite verificar se as cláusulas contratuais foram efetivamente cumpridas com base em dados concretos. Dessa forma, o modelo garante uma representação clara e rastreável dos compromissos estabelecidos em um SLA, vinculando cada cláusula a métricas específicas e suas respectivas medições.

Figura 19. SLA em formato UML.



Fonte: Elaborado pelo autor.

10. ACORDO DE NÍVEL DE SERVIÇO EM XML.

Abaixo encontra-se o contrato SLA no formato XML (eXtensible Markup Language) utilizado para facilitar a divulgação e compartilhamento do documento entre diferentes

plataformas. Todo o conteúdo está organizado de maneira fácil e intuitiva, utilizando tags de marcação para a delimitação das cláusulas.

```
<acordo_nivel_servico>
  <titulo>Contrato de Acordo de Nível de Serviço (SLA)</titulo>
  <partes_envolvidas>
        <prestador>Responsável técnico pela gestão e monitoramento da rede descrita neste documento.</prestador>
        <usuarios>Todos os indivíduos e sistemas que fazem uso da rede computacional monitorada.</usuarios>
  </partes_envolvidas>
  <clausulas>
        <clausula numero="1">
        <titulo>OBJETIVO</titulo>
        <descricao>Este Acordo de Nível de Serviço tem como objetivo definir os compromissos, garantias e responsabilidades relativos à prestação dos serviços da rede, com base nos recursos disponíveis, desempenho esperado e nível de suporte técnico oferecido. Este documento visa assegurar a transparência entre o prestador e os usuários da rede.</descricao>
        </clausula>
        <clausula numero="2">
        <titulo>ESCOPO</titulo>
        <descricao>O presente SLA aplica-se à infraestrutura de rede local composta por: um notebook (servidor principal, com Zabbix instalado); uma máquina virtual (clientes monitorados); um smartphone (host não monitorado); um roteador doméstico (gateway de acesso à internet). Estes dispositivos fazem parte de uma rede residencial com fins educacionais e de teste.</descricao>
        </clausula>
        <clausula numero="3">
        <titulo>DISPONIBILIDADE DA REDE</titulo>
        <descricao>Fica estabelecido que a rede deverá manter um índice mínimo de 95% de disponibilidade mensal, exceto em casos de: falhas de energia elétrica; manutenção programada; fatores externos que impeçam a operação da infraestrutura.</descricao>
        </clausula>
        <clausula numero="4">
        <titulo>TEMPO DE RESPOSTA DO SUPORTE TÉCNICO</titulo>
        <descricao>Ocorrendo incidentes ou falhas, o tempo máximo de resposta do responsável técnico deverá ser de: até 30 minutos para incidentes críticos (ex: perda total de conectividade); até 2 horas para incidentes de médio impacto; até 6 horas para solicitações de baixa prioridade ou informativas.</descricao>
        </clausula>
        <clausula numero="5">
```

```
        <titulo>SERVIÇOS MONITORADOS</titulo>
        <descricao>Estão incluídos neste SLA os seguintes serviços: monitoramento de disponibilidade e desempenho dos hosts monitorados (VMs); análise de tráfego de rede (bits in/out); verificação de leitura/escrita em disco; acesso à internet e conectividade entre dispositivos internos.</descricao>
        </clausula>
        <clausula numero="6">
        <titulo>PENALIDADES E NÃO CONFORMIDADES</titulo>
        <descricao>Em caso de descumprimento recorrente deste SLA, o prestador poderá ser advertido formalmente, considerando que este é um ambiente de testes. Este documento não implica em obrigações financeiras, mas sim em compromissos acadêmicos e operacionais.</descricao>
        </clausula>
        <clausula numero="7">
        <titulo>SEGURANÇA DA REDE</titulo>
        <descricao>O ambiente deverá obedecer aos seguintes requisitos de segurança: acesso restrito via autenticação local (Basic Auth &amp;amp; SSH); monitoramento contínuo de portas e serviços via Zabbix; utilização de firewall ativo nas máquinas monitoradas; uso de NAT para isolamento da rede local.</descricao>
        </clausula>
        <clausula numero="8">
        <titulo>MONITORAMENTO E MÉTRICAS</titulo>
        <descricao>A verificação dos parâmetros estabelecidos será feita através da ferramenta Zabbix, instalada no host principal. Serão gerados relatórios semanais com métricas de desempenho, alertas e gráficos. O histórico de eventos será utilizado para avaliação de conformidade com este SLA.</descricao>
        </clausula>
        <clausula numero="9">
        <titulo>VIGÊNCIA DO ACORDO</titulo>
        <descricao>O presente acordo entra em vigor na data de implantação do monitoramento e terá validade de 6 (seis) meses, podendo ser revisado ou renovado conforme necessidade. E por estarem de acordo, as partes consideram este SLA como referência para a operação, avaliação e melhoria contínua da rede monitorada.</descricao>
        </clausula>
    </clausulas>
    <data_local>Florianópolis, 20 de Abril de 2025.</data_local>
</acordo_nivel_servico>
```

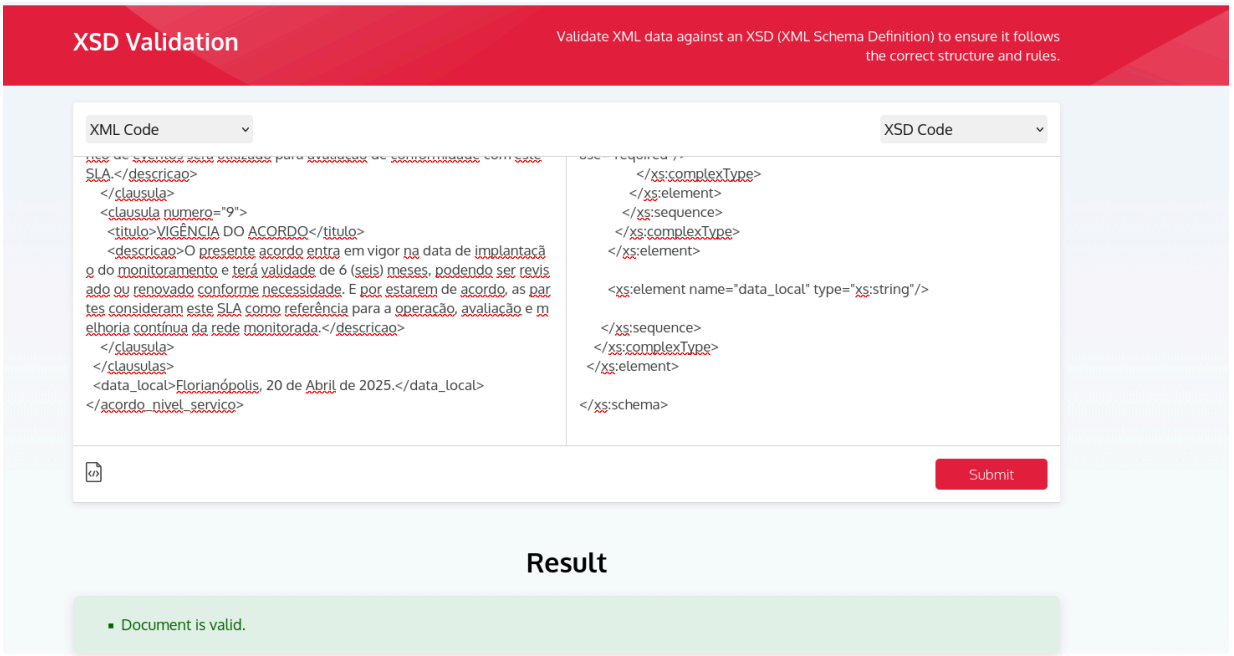
10.1. SCHEMA PARA VALIDAÇÃO DO XML E RESULTADO.

O Bloco de código abaixo apresenta o Schema de validação (XSD) com base no modelo em XML, que é utilizado em plataformas de validação.

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema">

 <xs:element name="acordo_nivel_servico">
        <xs:complexType>
        <xs:sequence>
        <xs:element name="titulo" type="xs:string"/>

        <xs:element name="partes_envolvidas">
        <xs:complexType>
        <xs:sequence>
        <xs:element name="prestador" type="xs:string"/>
        <xs:element name="usuarios" type="xs:string"/>
        </xs:sequence>
        </xs:complexType>
        </xs:element>

        <xs:element name="clausulas">
        <xs:complexType>
        <xs:sequence>
        <xs:element name="clausula" maxOccurs="9">
                <xs:complexType>
                <xs:sequence>
                <xs:element name="titulo" type="xs:string"/>
                <xs:element name="descricao" type="xs:string"/>
                </xs:sequence>
                <xs:attribute name="numero" type="xs:positiveInteger"
use="required"/>
                </xs:complexType>
        </xs:element>
        </xs:sequence>
        </xs:complexType>
        </xs:element>

        <xs:element name="data_local" type="xs:string"/>

        </xs:sequence>
        </xs:complexType>
 </xs:element>

</xs:schema>
```

A validação foi realizada utilizando a plataforma https://www.utilities-online.info/xsdvalidation onde o XML foi submetido ao esquema XSD (XML Schema Definition) definido acima. O resultado retornado pela ferramenta confirmou que o XML está estruturalmente correto, sem erros de marcação ou violação de esquema:

Figura 20. Resultado da validação do SLA em XML

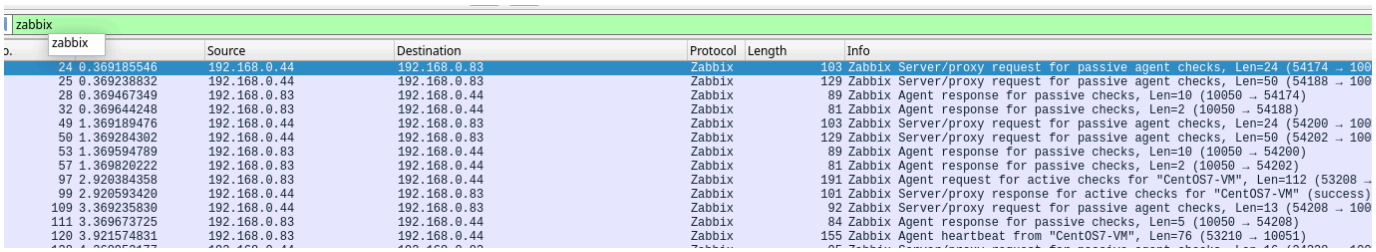


Fonte: Elaborado pelo autor.

11. RESULTADOS/PACOTES WIRESHARK.

Além dos testes iniciais apresentados na Seção 6, foram realizados testes adicionais utilizando o Wireshark com o objetivo de verificar e validar a comunicação entre os componentes do Zabbix durante o monitoramento da rede. Essa etapa é essencial para garantir que o tráfego de dados entre o Zabbix Server e o Zabbix Agent ocorra de forma adequada e que os pacotes estejam sendo trocados corretamente.

Figura 21. Captura dos pacotes trocados entre o Zabbix Server e o Zabbix Agent.

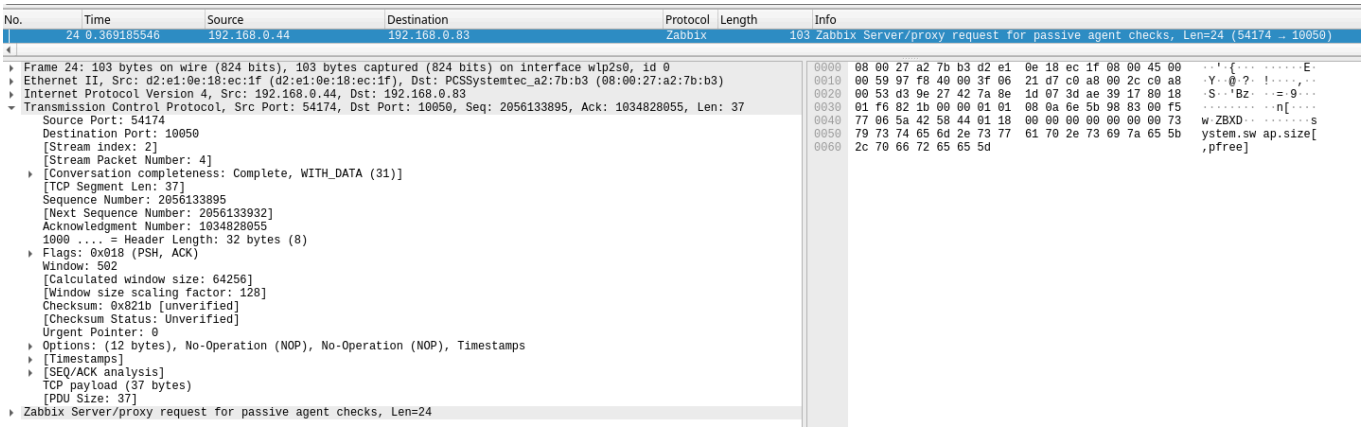


Fonte: Elaborado pelo autor.

A Figura 22 mostra o cabeçalho detalhado de um dos pacotes enviados pelo servidor Zabbix para o agente. Nele é possível identificar informações como:

- Protocolo utilizado (TCP);
- Porta de origem e de destino (normalmente porta 10050 para o agente Zabbix);
- Endereços IP de origem e destino;
- Tamanho do pacote;
- Sequência de dados enviados.

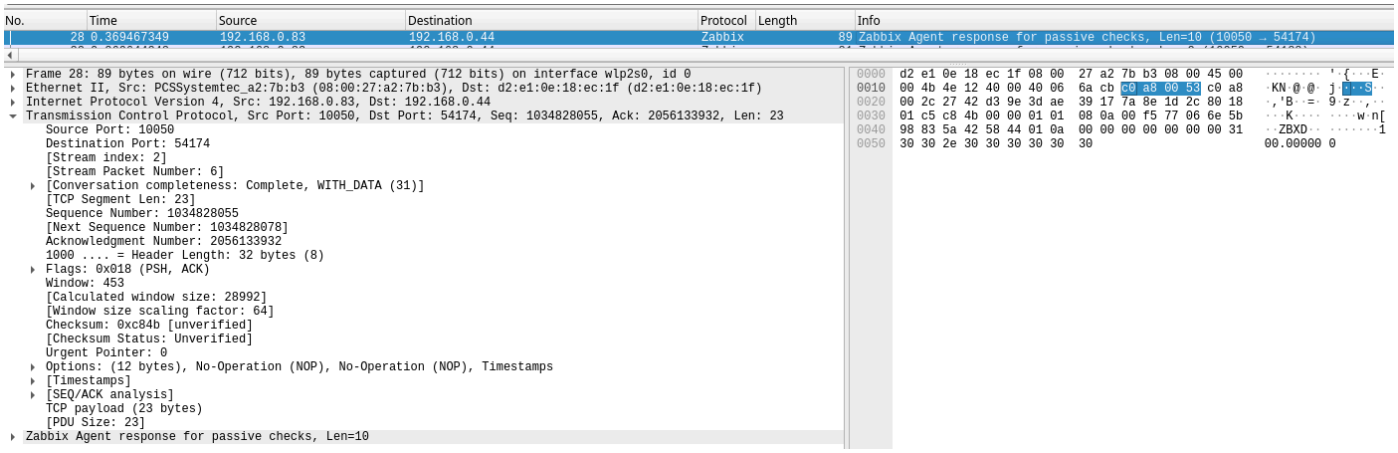
Figura 22. Cabeçalho do pacote de requisição enviado pelo Zabbix Server ao Zabbix Agent.



Fonte: Elaborado pelo autor.

A Figura 23 evidencia a estrutura de um pacote de resposta enviado pelo agente ao servidor, confirmando a entrega dos dados solicitados e o correto funcionamento da comunicação bidirecional.

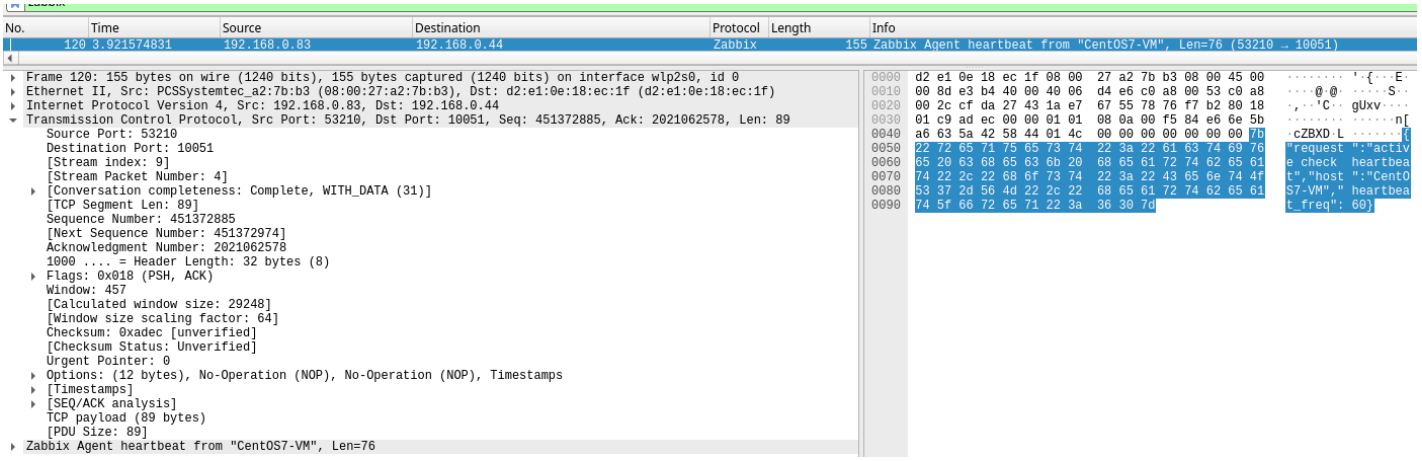
Figura 23. Estrutura do pacote de resposta do Zabbix Agent ao Zabbix Server.



Fonte: Elaborado pelo autor.

Por fim, a Figura 24 demonstra a análise de desempenho da troca de pacotes, permitindo observar o tempo de resposta entre requisição e resposta, o que é fundamental para avaliar a eficiência do monitoramento.

Figura 24. Cabeçalho de resposta da verificação de ativação do Zabbix Agent.



Fonte: Elaborado pelo autor.

Foram observados pacotes como:

- Zabbix Server/proxy request for passive agent checks
- Zabbix Agent response for passive checks
- Zabbix Agent heartbeat from "CentOS7-VM"

Esses pacotes evidenciam que o agente está ativo, recebendo e respondendo às requisições de checagem do servidor. A troca contínua de informações permite que os dados de disponibilidade, uso de CPU, memória, disco e rede sejam atualizados e exibidos na interface web do Zabbix. O arquivo com as medições será enviado em anexo, juntamente com o relatório.

12. MEDIÇÕES CONFORME O ACORDO DE NÍVEL DE SERVIÇO (SLA).

Resumo das métricas:

Tabela 3. Resultado das medições das métricas

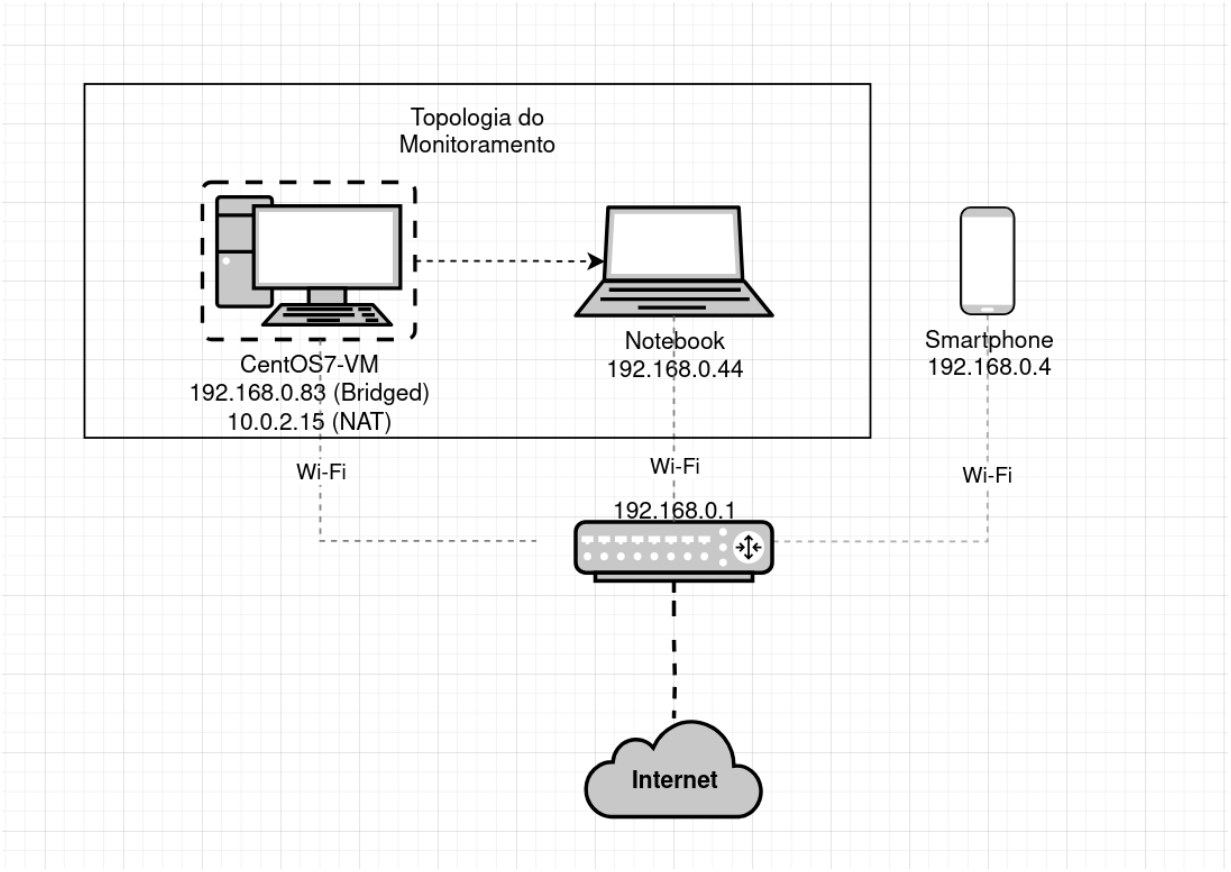
Métrica	Resultado
Uptime superior a 95% (Cláusula 3)	Respeitada
Uso de CPU (Cláusula 8)	Violada

Conectividade Interna (Cláusula 5 Item 1)	Respeitada
Tráfego de Rede (Cláusula 5 Item 2)	Respeitada
Uso de disco (Cláusula 5 Item 3)	Respeitada

Fonte: Elaborado pelo autor.

12.1. Uptime Superior a 95%.

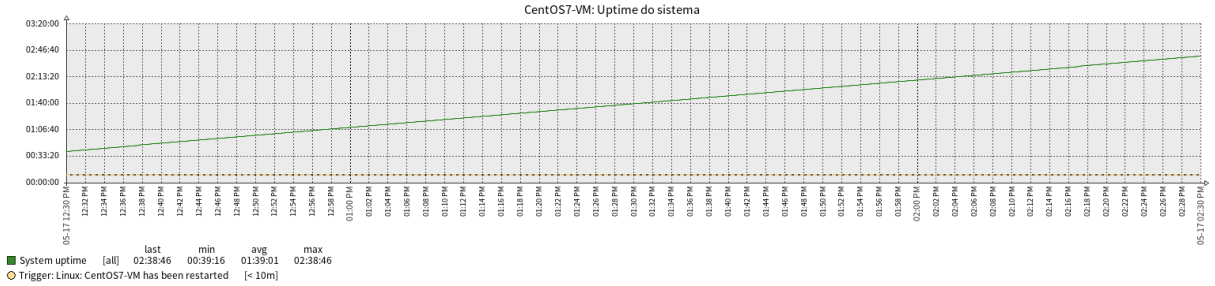
Figura 25. Topologia métrica de Uptime.



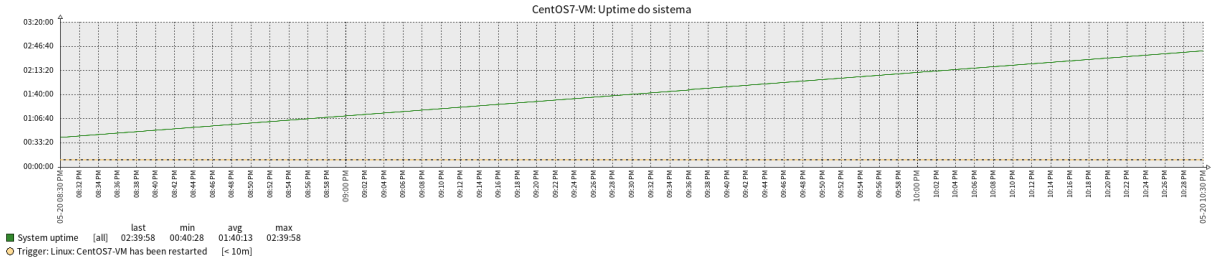
Fonte: Elaborado pelo autor.

17/05/2025 - 12:30h até 14:30h

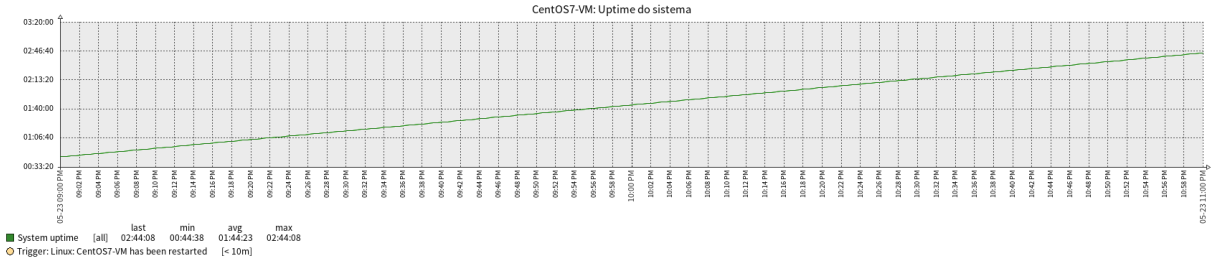
Ficou rodando de 11h a 18h no total



20/05/2025 - 20:30h até 22:30h



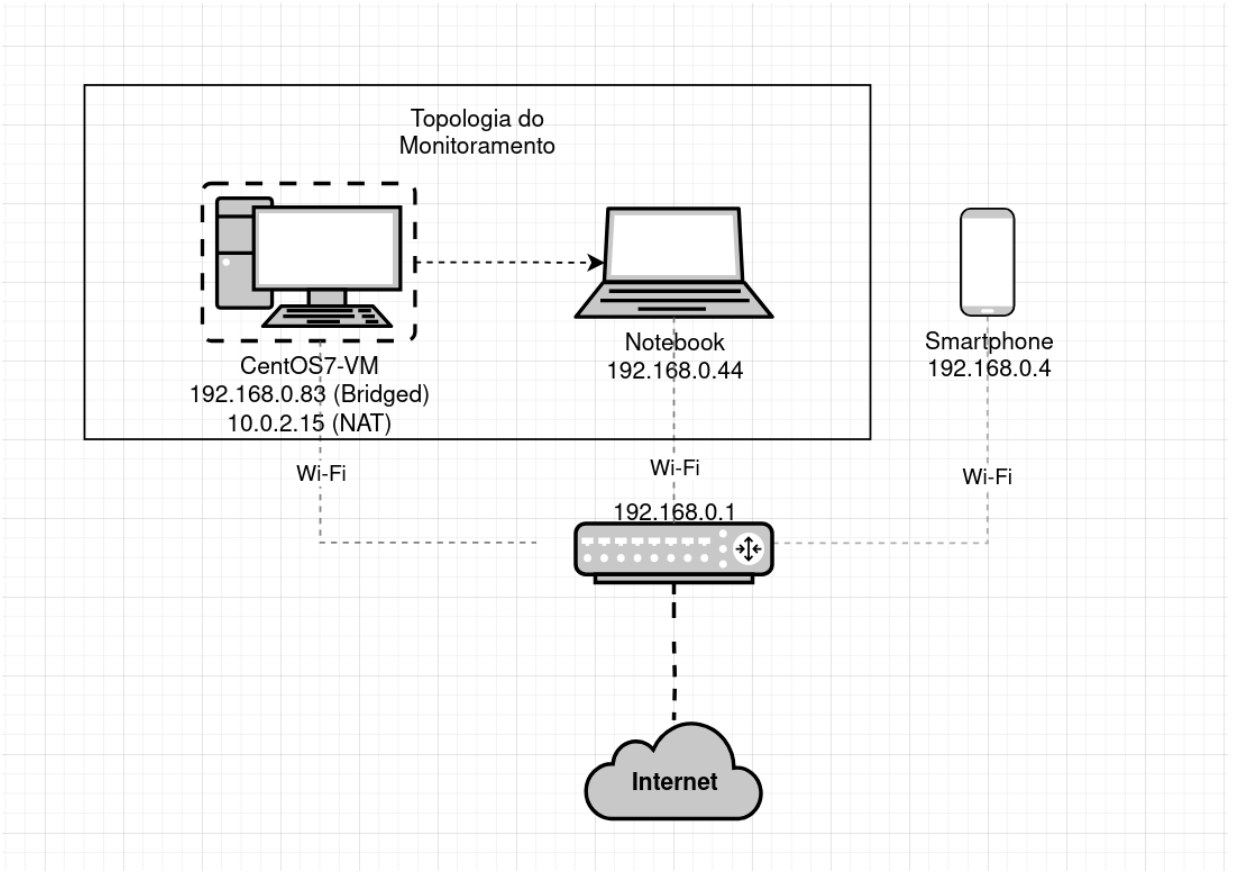
23/05/2025 - 21:00h até 23:00h



Em todas as sessões, o host permaneceu ativo e disponível, resultando em uptime superior a **95%**, conforme exigido pela Cláusula 3 do SLA.

12.2. Uso de CPU.

Figura 25. Topologia métrica uso de CPU.



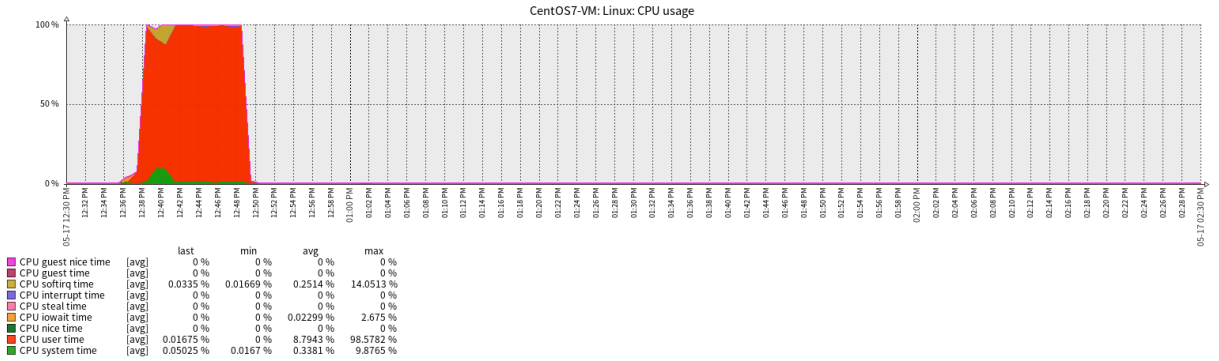
Fonte: Elaborado pelo autor.

17/05/2025 - 12:30h até 14:30h

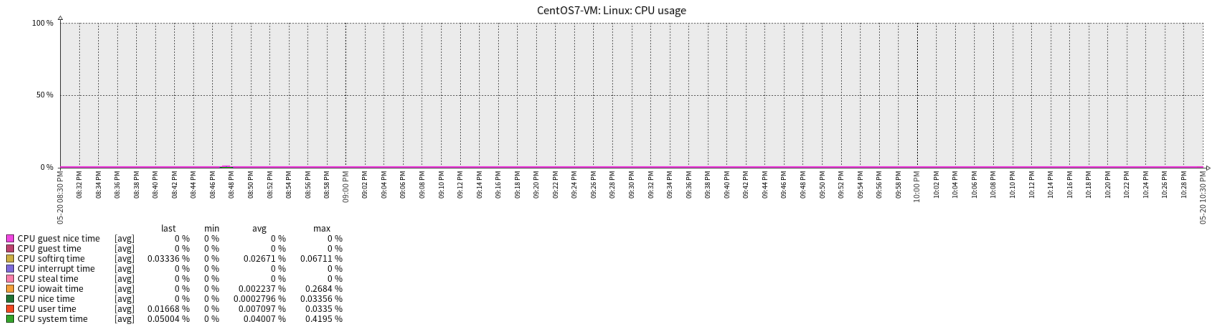
Rodei o comando abaixo para estresse da CPU:

```
for i in {1..4}; do yes > /dev/null & done; sleep 30; killall yes
```

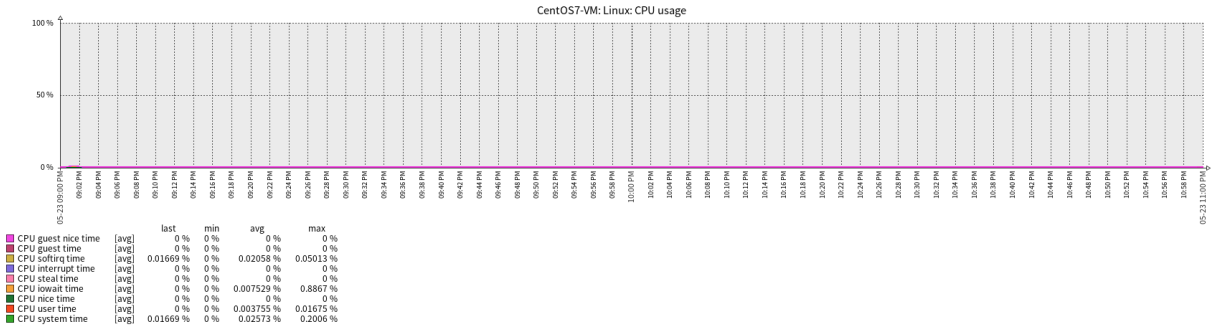
Este comando manteve a CPU em 100% de utilização por cerca de 5 minutos durante a janela de 17/05/2025:



20/05/2025 - 20:30h até 22:30h



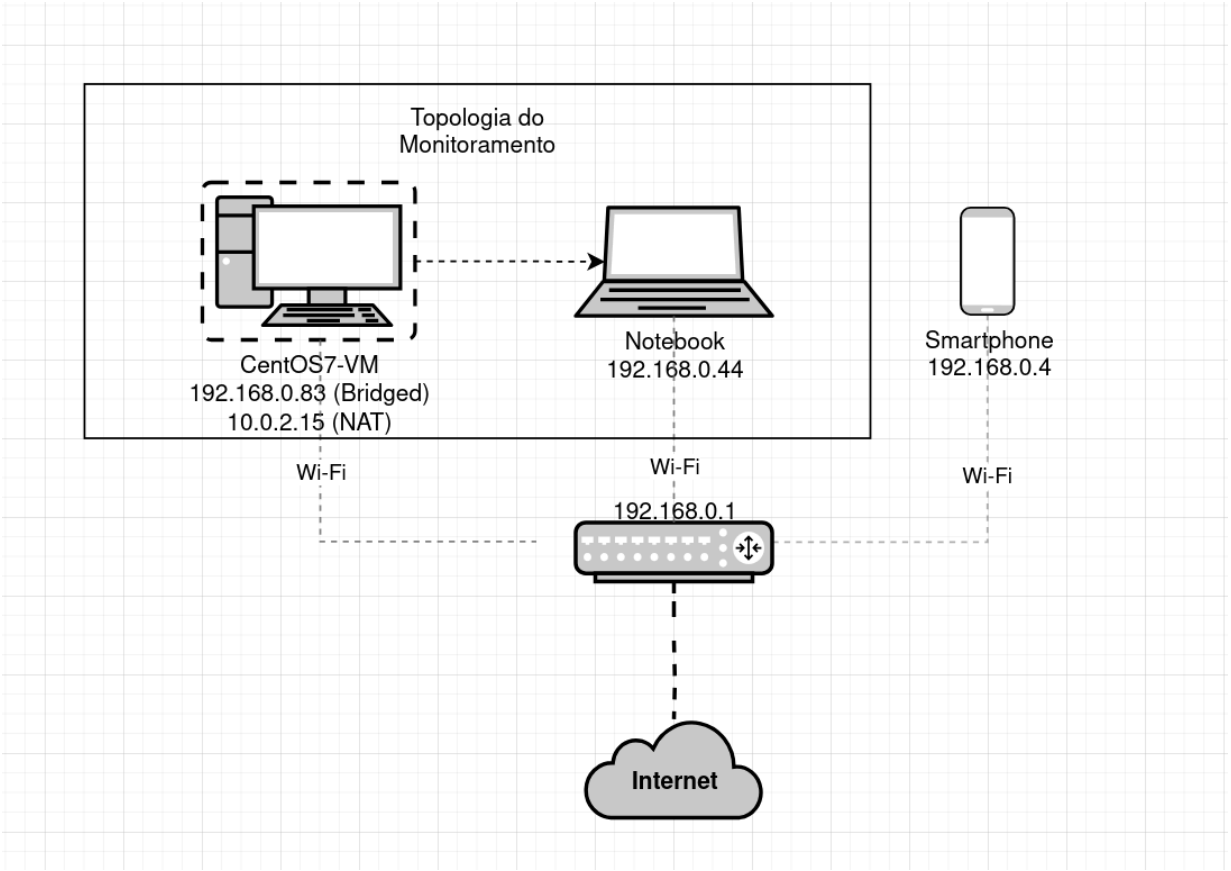
23/05/2025 - 21:00h até 23:00h



Em momentos de estresse, o SLA foi violado, pois não havia garantia de limitação de uso máximo de CPU. No entanto, fora desses momentos, a utilização manteve-se estável.

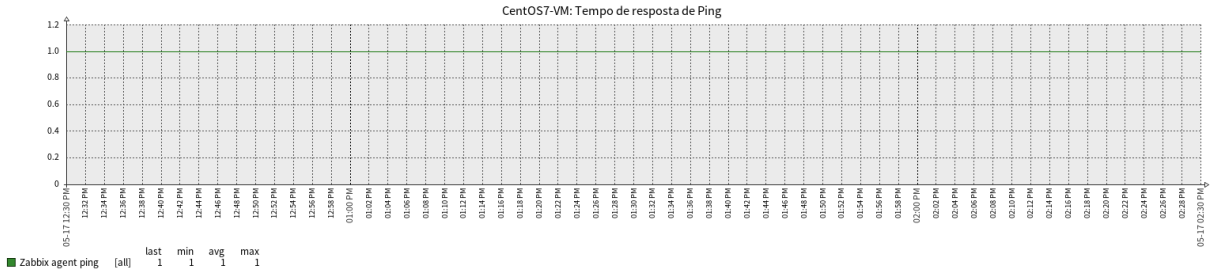
12.3. Conectividade Interna.

Figura 25. Topologia métrica conectividade interna.

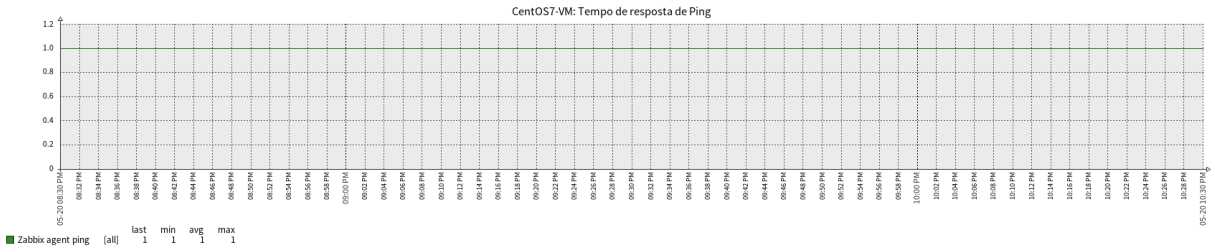


Fonte: Elaborado pelo autor.

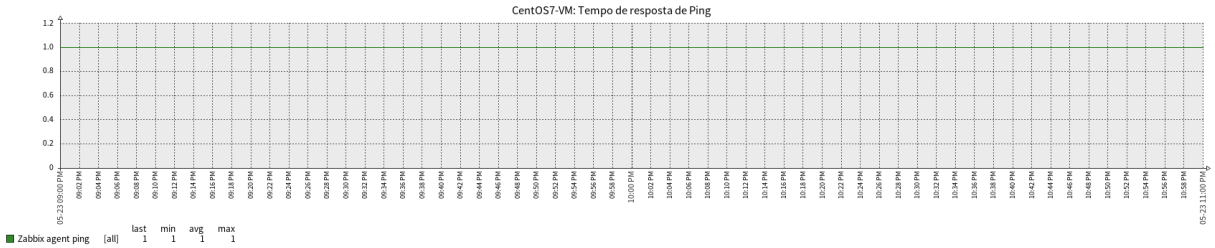
17/05/2025 - 12:30h até 14:30h



20/05/2025 - 20:30h até 22:30h



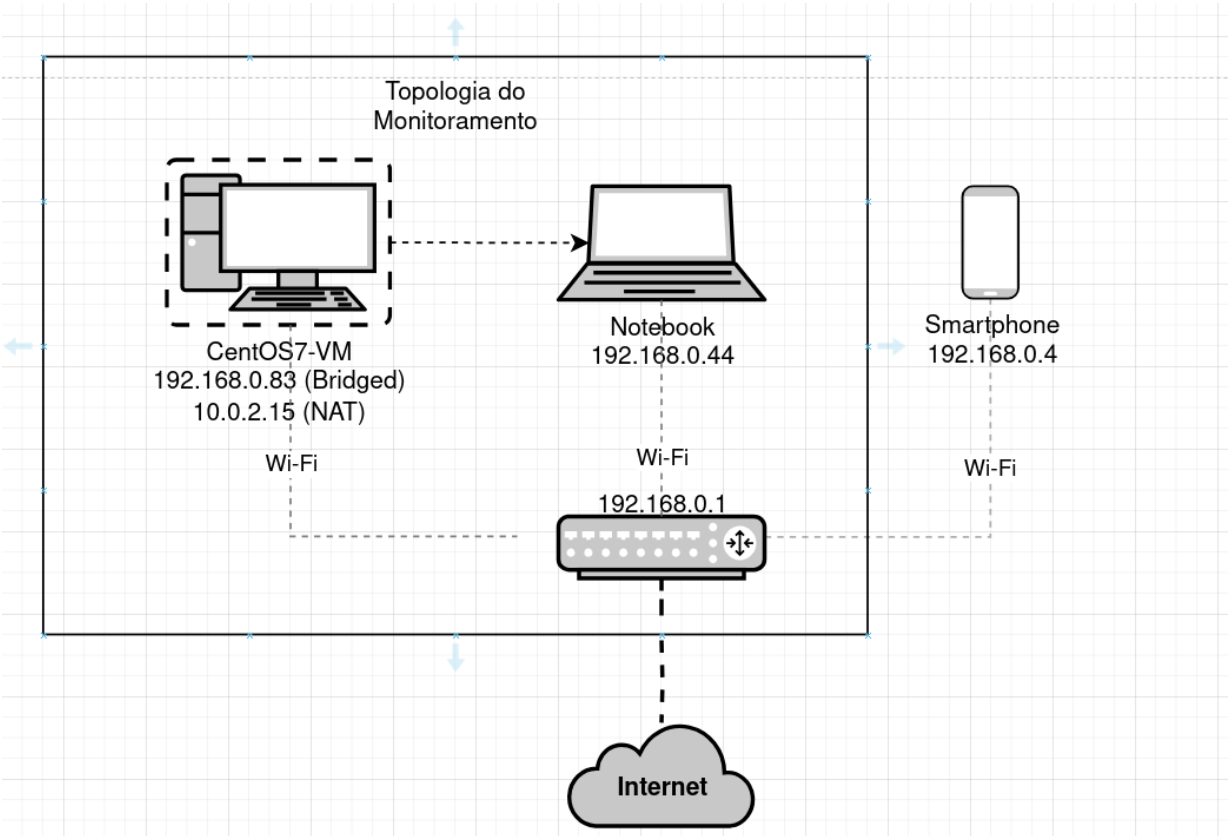
23/05/2025 - 21:00 até 23:00h



Nenhuma perda de pacotes foi observada, indicando conectividade estável, conforme estabelecido no SLA.

12.4. Tráfego de Rede.

Figura 25. Topologia métrica tráfego de rede.

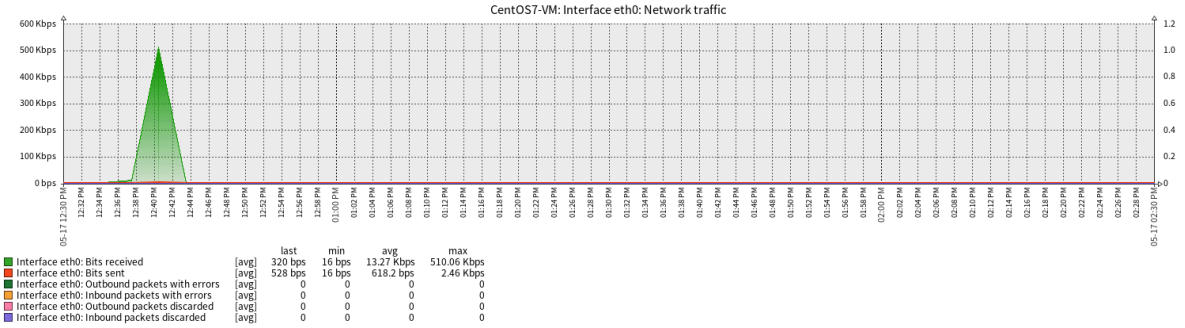


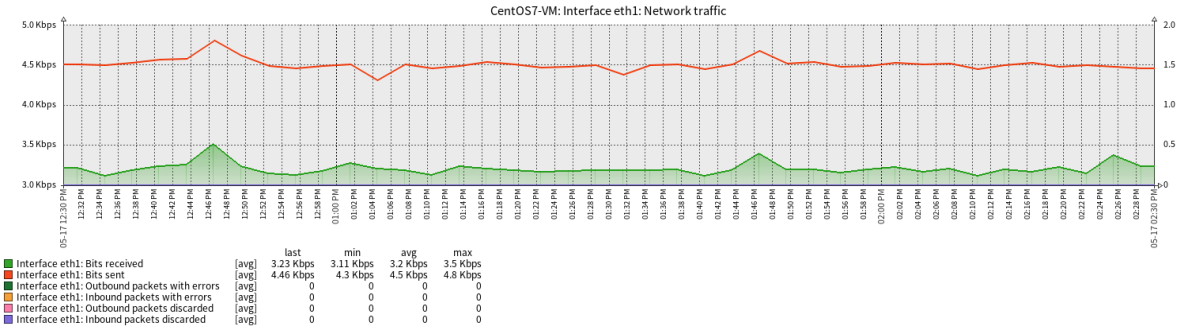
Fonte: elaborado pelo autor.

17/05/2025 - 20:30 até 22:30

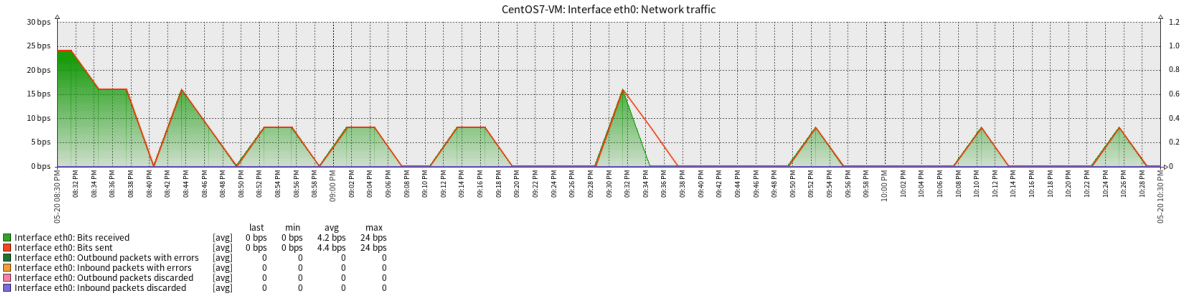
Para gerar tráfego, realizamos downloads via yum nas sessões monitoradas:

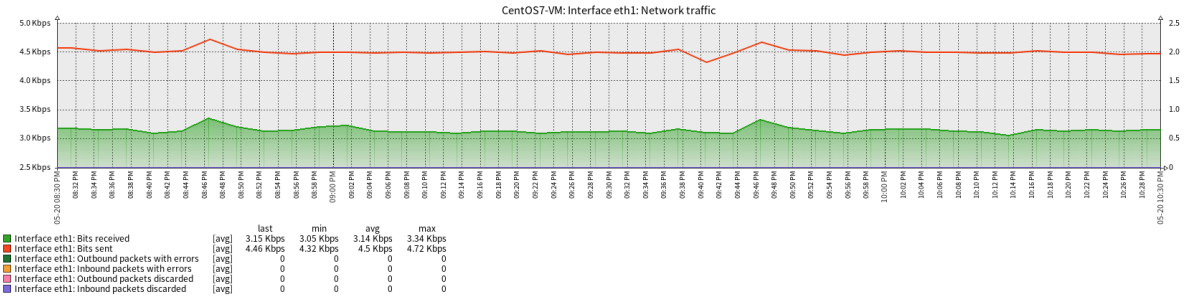
```
Sudo yum install htop -y
Sudo yum install wget -y
```



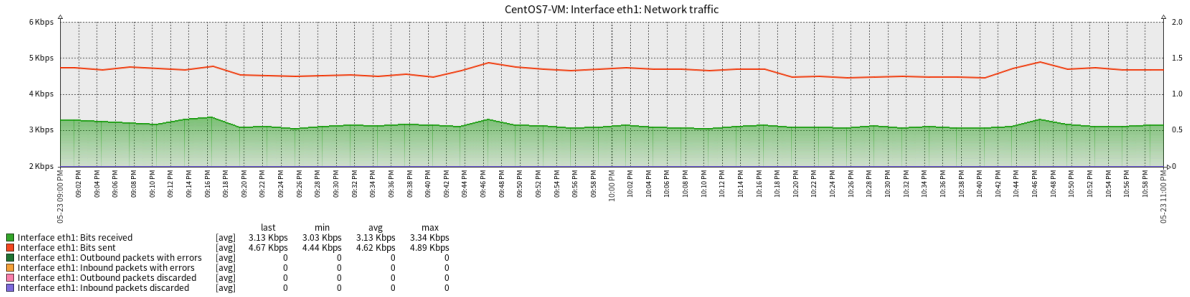


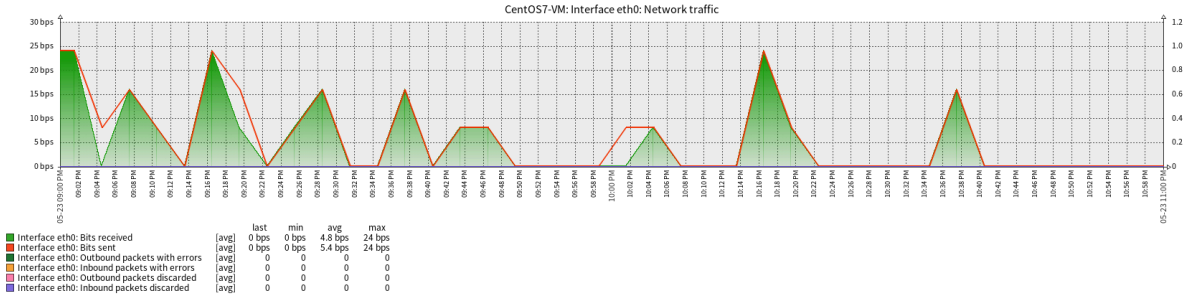
20/05/2025 - 20:30 até 22:30





23/05/2025 - 21:00h até 23:00h

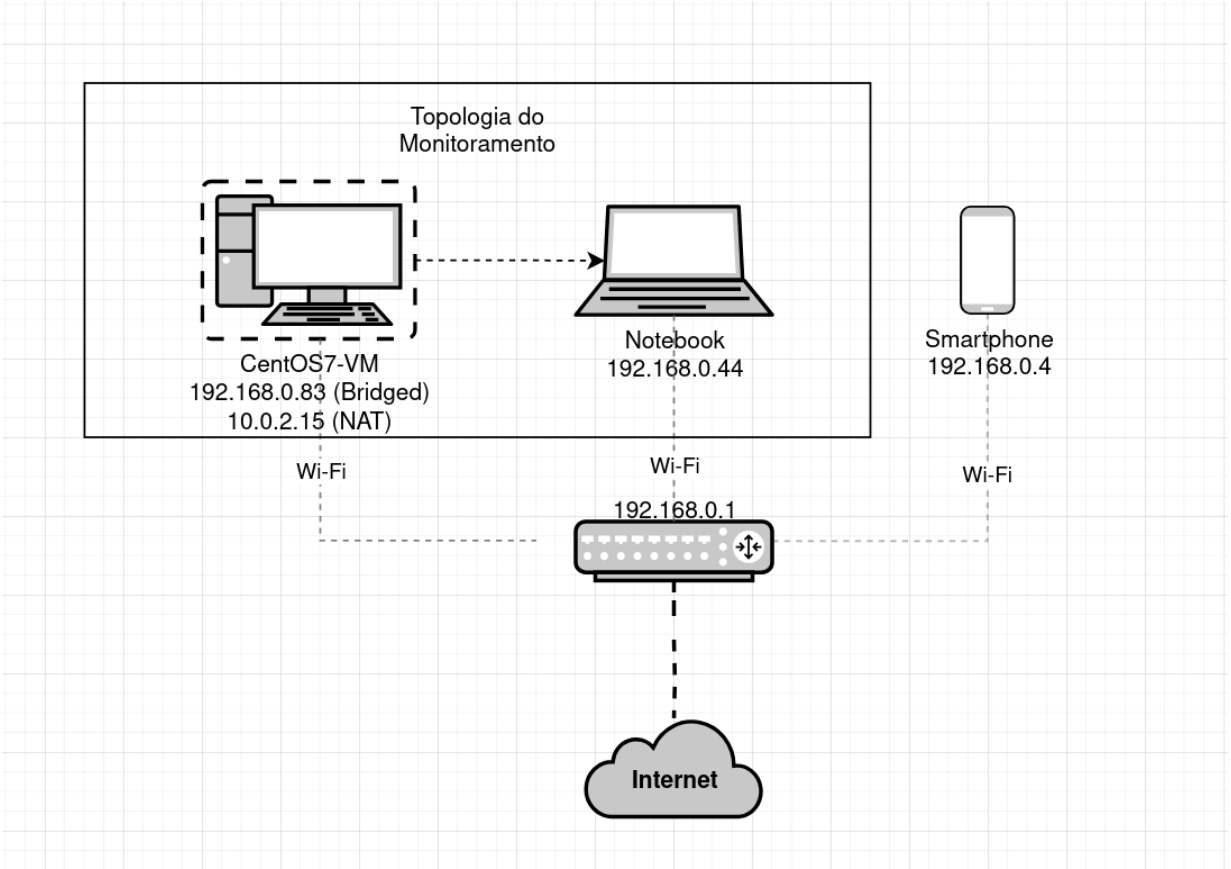




Os gráficos de bits enviados e recebidos confirmaram a elevação da taxa de transferência nesses períodos, cumprindo a medição exigida pela cláusula do SLA.

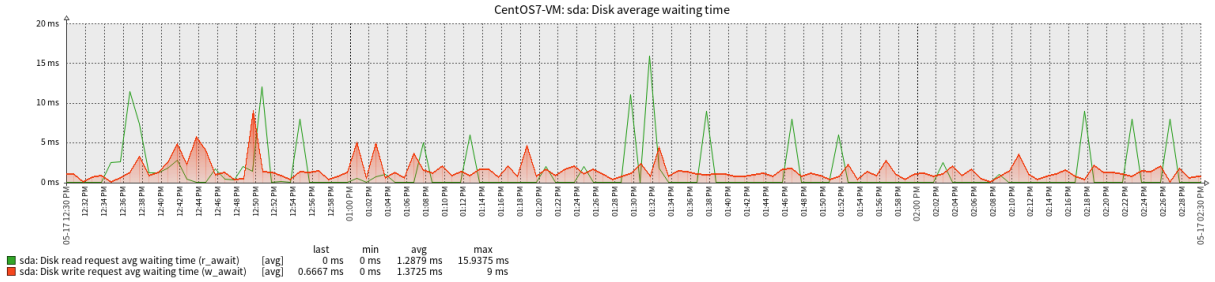
12.5. Uso de disco.

Figura 25. Topologia métrica uso de disco.

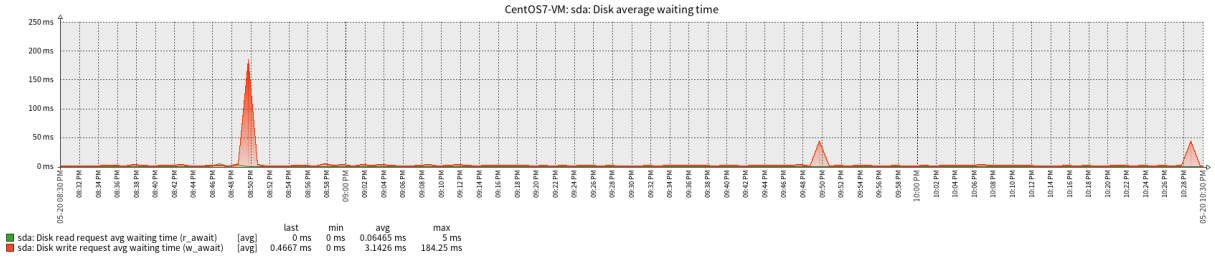


Fonte: Elaborado pelo autor.

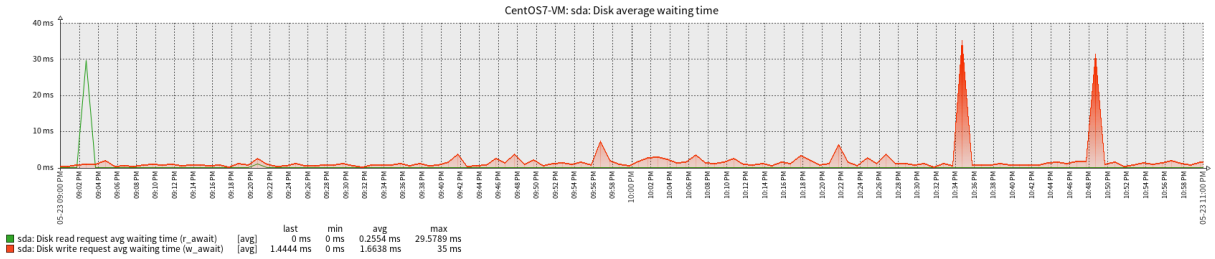
17/05/2025 - 12:30h até 14:30h



20/05/2025 - 20:30h até 22:30h



23/05/2025 - 21:00h até 23:00h



O espaço disponível permaneceu acima de 30%, dentro dos parâmetros aceitáveis para o ambiente de testes.

De modo geral, as medições realizadas confirmaram que a infraestrutura monitorada atende aos requisitos estabelecidos no SLA, com exceção dos picos de utilização de CPU durante testes de estresse. A conectividade interna, a disponibilidade e a estabilidade dos serviços demonstraram estar adequadas para o ambiente proposto.

REFERÊNCIAS

AMAZON WEB SERVICES. O que é SLA? - Explicação sobre acordos de nível de serviço - AWS. Disponível em: https://aws.amazon.com/pt/what-is/service-level-agreement/. Acesso em: 20 abr. 2025.

INSIGHTS, The Expert. O que é Acordo de Nível de Serviço? Como fazer? + Exemplo. Zendesk, [s.d.]. Disponível em: https://www.zendesk.com.br/blog/o-que-e-acordo-de-nivel-de-servico/#. Acesso em: 20 abr. 2025.

MAXFIELD, Fredrik. Zabbix install with Docker and Portainer. Medium, 2019. Disponível em: https://medium.com/@fredrik.maxfield/simplified-zabbix-deployment-step-by-step-with-docker-and-portainer-19e85c08a65b. Acesso em: 20 abr. 2025.

ZABBIX. Installation from containers. Zabbix Documentation. Disponível em: https://www.zabbix.com/documentation/current/en/manual/installation/containers. Acesso em: 20 abr. 2025.