



Universidade Federal de Santa Catarina
Departamento de Informática e Estatística
Administração e Gerência de Redes de Computadores

Caetano Colin Torres

RELATÓRIO DO TRABALHO PRÁTICO - GERÊNCIA DE REDES

Florianópolis-SC, Brasil
2022

Resumo

Este trabalho prático é um trabalho acadêmico com teor avaliativo realizado na disciplina de Administração e Gerência de Redes da Universidade Federal de Santa Catarina. Neste trabalho será instalado uma ferramenta de gerência de redes, o Zabbix e será configurado dispositivos agentes que serão monitorados com diversas medições. Além disso, será esboçado um acordo de nível de serviço (SLA) com cláusulas e métricas que serão medidas posteriormente através da ferramenta de gerência de redes escolhida. Também será usado o Wireshark para gerência de redes, capturando tráfego e auxiliando na depuração da rede TCP/IP.

SUMÁRIO

1. DESCRIÇÃO DA CONFIGURAÇÃO DOS RECURSOS E DA REDE	4
2. TOPOLOGIA DA REDE MONITORADA	4
3. FERRAMENTAS UTILIZADAS PARA GERÊNCIA	5
4. INSTALAÇÃO E CONFIGURAÇÃO DO ZABBIX	6
5. MEDIÇÕES INICIAIS DO ZABBIX	10
5.1 Wireshark para gerência de redes	14
6. QUESTIONÁRIO DE SATISFAÇÃO DOS USUÁRIOS	15
6.1. Como você classificaria o desempenho geral da rede?	16
6.2. O quão estável é a rede? E a disponibilidade dos serviços?	17
6.3. Classifique em relação ao tempo gasto para que o suporte técnico resolva eventuais problemas	18
6.4. Como é a qualidade dos serviços providos pelo suporte técnico?	19
6.5. Como é a qualidade do acesso à rede externa (Internet)?	20
6.6. Como é a qualidade dos serviços prestados?	21
6.7. Como é a qualidade da segurança da rede?	22
7. ACORDO DE NÍVEL DE SERVIÇO - SLA	22
7.1 Visão Geral	22
7.2 Sumário Executivo	23
7.3 Parâmetros e Métricas de Desempenho do Serviço Contratado	24
7.4 Escopo de Serviço	24
7.5 Sanções e Penalidades	24
7.6 Responsabilidades Mútuas	25
8. ACORDO DE NÍVEL DE SERVIÇO EM UML	26
9. ACORDO DE NÍVEL DE SERVIÇO EM XML	26
10. VALIDAÇÃO DO XML	33
11. CONFIGURAÇÕES ADICIONAIS PARA SNMP	35
12. EXTENSÃO DA MIB-2 SNMP	35
12.1. Criando o novo objeto e configurando o SNMP	35
12.2. Configuração no Zabbix do item estendido	39
12.3. Modificação do Contrato	41
13. MONITORAMENTO DAS MÉTRICAS DO SLA	41
13.1. Número de Threads	41
13.2. Uso da Memória RAM	43
13.3. Tráfego na Interface de Rede	45
13.4. Disponibilidade do Servidor	47
13.5. Número de Inodes	49
13.6. Número de conexões na porta 443 (MIB Estendida)	50
REFERÊNCIAS	53

1. DESCRIÇÃO DA CONFIGURAÇÃO DOS RECURSOS E DA REDE

A rede será composta de 3 máquinas, um notebook principal que será o hospedeiro do *Zabbix* e também o processo gerente, uma *workstation* com rede cabeada via cabo UTP, que será um processo agente, e um outro notebook conectado na rede via *Wi-fi* que também será um processo gerente. Usando pelo menos 2 sistemas operacionais diferentes. A rede é uma rede local de uso pessoal, onde teremos 3 máquinas com diferentes capacidades de processamento disponíveis para uso. Além dessas 3 máquinas, temos um modem TP-Link que provê o acesso à rede internet via infraestrutura da provedora de internet.

1.1 CONFIGURAÇÃO DAS MÁQUINAS

Hostname	Tipo	Sistema Operacional	Endereço IP	Tipo de conexão	RAM	Processador
Notebook 1	Gerente/Hospedeiro	Ubuntu	192.168.178.230 (Via DHCP)	Wi-fi	16GB	Intel i7 1.8GHz
Workstation	Agente	Windows	192.168.178.231 (Via DHCP)	UTP	16GB	Ryzen 5 2.3GHz
Notebook 2	Agente	Ubuntu	192.168.178.211 (Via DHCP)	Wi-fi	4GB	Intel i5 1.5GHz

Tabela 1. Configuração dos dispositivos da Rede Gerenciada

2. TOPOLOGIA DA REDE MONITORADA

Na topologia representada na imagem abaixo, vemos listado a máquina *Notebook1*, o processo gerente e também com métricas sendo monitoradas pelo *Zabbix*, a máquina *Notebook2*, um host agente que está sendo monitorado e o host *Workstation*, que é outro host sendo monitorado. O roteador TP-Link está representado no centro da topologia, provendo acesso para a rede externa através de NAT. Também estão representados outros dispositivos na rede local que não estão sendo monitorados por um telefone.

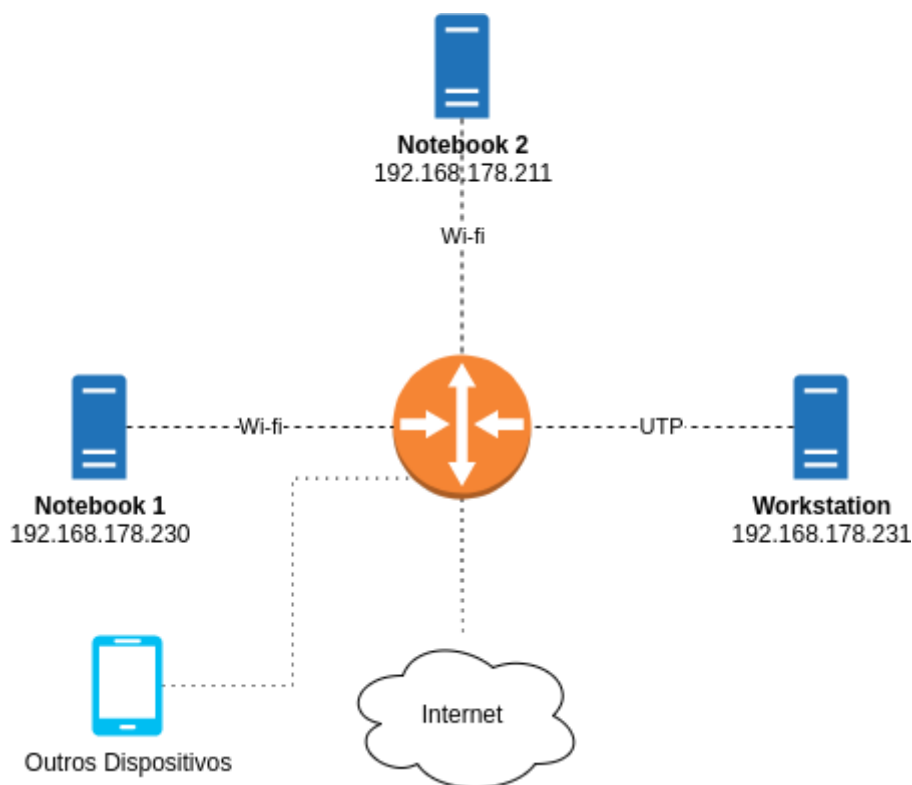


Figura 1. Topologia da Rede Gerenciada.

3. FERRAMENTAS UTILIZADAS PARA GERÊNCIA

O *Zabbix*, ferramenta de gerência escolhida, é uma ferramenta de software de código aberto para monitorar a infraestrutura de TI, como redes, servidores, máquinas virtuais e serviços em nuvem. Ele será usado para coletar as métricas que serão analisadas no SLA. Também foi usado o *Wireshark*, programa que analisa o tráfego de rede, para capturar o tráfego em algumas partes deste relatório. O *Zabbix* possui suporte nativo para *SNMP* (*Simple Network Management Protocol*). O *Wireshark* foi usado para capturar o tráfego *SNMP* e analisar a operação de troca de dados entre diferentes *hosts*, verificando a confiabilidade do sistema. Nas próximas seções iremos descrever o funcionamento e configuração das ferramentas. O *Zabbix Agent* é uma ferramenta poderosa, que instala um processo agente que enviará dados para o servidor central (processo gerente). O *Zabbix* contempla vários templates e regras de descoberta para esses agentes, facilitando muito o processo de instalação e configuração na gerência de redes. Todavia, em dispositivos como switches, roteadores e impressoras, que possuem menos versatilidade e capacidade de abstração de monitoramento, devemos configurar o *SNMP* para trocar dados, na maioria das vezes.

4. INSTALAÇÃO E CONFIGURAÇÃO DO ZABBIX

Instalando Zabbix Server, Zabbix Frontend e Zabbix Agent. O Zabbix Server tem a finalidade de configurar o backend do servidor, responsável pelo banco de dados e tratamento dos dados que chegam dos agentes. O Zabbix Frontend estabelece a interface com o usuário para configurar os hosts e os itens monitorados. E, o Zabbix Agent é instalado nas máquinas monitoradas e serve para enviar os dados para o ambiente central.

- Instalando os pacotes necessários:

```
wget
https://repo.zabbix.com/zabbix/6.0/ubuntu/pool/main/z/zabbix-release/
zabbix-release_6.0-1+ubuntu$(lsb_release -rs)_all.deb

sudo dpkg -i zabbix-release_6.0-1+ubuntu$(lsb_release
-rs)_all.deb

sudo apt update

sudo apt -y install zabbix-server-mysql zabbix-frontend-php
zabbix-apache-conf zabbix-sql-scripts zabbix-agent
```

- Configurando o banco de dados

Nosso banco de dados será configurado com **rootDBpass** como a senha **root** e **zabbixDBpass** como a senha do zabbix.

```
sudo apt install software-properties-common -y

curl -LsS -O
https://downloads.mariadb.com/MariaDB/mariadb_repo_setup
sudo bash mariadb_repo_setup --mariadb-server-version=10.6

sudo apt update

sudo apt -y install mariadb-common mariadb-server-10.6
mariadb-client-10.6
```

- Deve-se colocar o *MariaDB* para rodar como serviço no *Linux*.

```
sudo systemctl start mariadb  
sudo systemctl enable mariadb
```

- Agora devemos configurar o acesso ao banco de dados:

```
sudo mysql_secure_installation  
-----  
Enter current password for root (enter for none): Press Enter  
Switch to unix_socket authentication [Y/n] y  
Change the root password? [Y/n] y  
New password: <Enter root DB password>  
Re-enter new password: <Repeat root DB password>  
Remove anonymous users? [Y/n]: Y  
Disallow root login remotely? [Y/n]: Y  
Remove test database and access to it? [Y/n]: Y  
Reload privilege tables now? [Y/n]: Y
```

- Após a configuração de acesso, vamos criar o banco de dados através da linguagem *SQL*.

```
sudo mysql -uroot -p'rootDBpass' -e "create database zabbix  
character set utf8mb4 collate utf8mb4_bin;"  
  
sudo mysql -uroot -p'rootDBpass' -e "grant all privileges on  
zabbix.* to zabbix@localhost identified by 'zabbixDBpass';"
```

- No próximo passo, iremos importar o esquema inicial do banco.

```
sudo zcat /usr/share/doc/zabbix-sql-scripts/mysql/server.sql.gz |  
mysql -uzabbix -p'zabbixDBpass' zabbix
```

Então, abrimos o arquivo `/etc/zabbix/zabbix_server.conf` com algum editor de texto e salvamos a senha `DBPassword=zabbixDBpass`

- Para configurar o Firewall no Zabbix Server, executamos os seguintes comandos:

```
ufw allow 10050/tcp
ufw allow 10051/tcp
ufw allow 80/tcp
ufw reload
```

Onde, 10050 é a porta do agente, 10051 é a porta servidor e 80 é a porta do frontend.

- Após liberar as portas, devemos iniciar os serviços do Zabbix como *daemon*:

```
sudo systemctl restart zabbix-server zabbix-agent
sudo systemctl enable zabbix-server zabbix-agent
```

Para configurar o *frontend* do Zabbix, deve-se editar o arquivo `/etc/zabbix/apache.conf`, é necessário adicionar o valor **php_value date.timezone America/Sao_Paulo** nesse arquivo e então executar os comandos:

```
sudo systemctl restart apache2
sudo systemctl enable apache2
```

Com isso, nosso *frontend* está pronto para ser acessado pelo endereço <http://192.168.178.230/zabbix>. Acessamos esse site e configuramos.



Figura 2. Tela de Configuração do Zabbix Frontend.

O único passo importante que vale ressaltar no relatório, é o passo de inserir a senha do banco dados na seção “Configure DB connection”. Depois basta efetuar o login no Zabbix usando as credenciais **Admin/zabbix**.

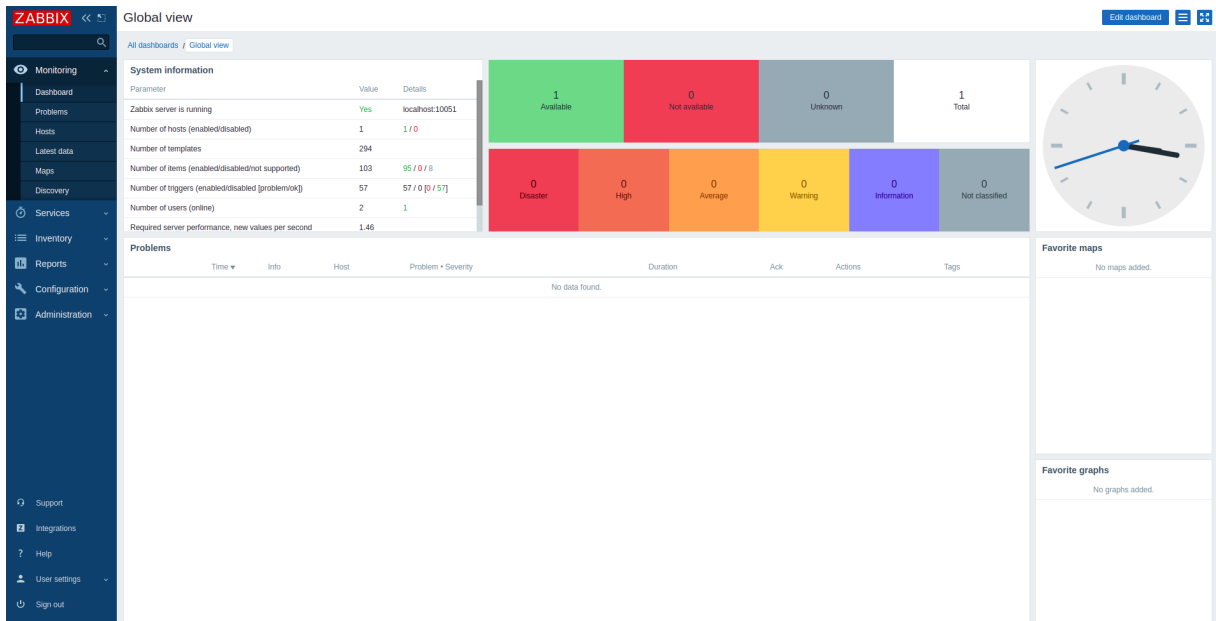


Figura 3. Tela Inicial do Zabbix após a configuração.

Para um primeiro teste, configuramos o *Zabbix Agent* no **Notebook1** (Zabbix Server) com a finalidade de testar a coleta de dados. Para isso, editamos o arquivo `/etc/zabbix/zabbix_agentd.conf` e adicionamos às seguintes linhas:

```
Server=192.168.178.230
Hostname=Notebook1
```

Então reiniciamos o serviço *zabbix-agent* usando o seguinte comando:

```
sudo systemctl restart zabbix-agent
sudo systemctl enable zabbix-agent
```

5. MEDIÇÕES INICIAIS DO ZABBIX

Após os passos executados na seção anterior, temos um ambiente de monitoramento *Zabbix* pronto para uso, como foi instalado um processo agente na máquina que hospeda o servidor do *Zabbix*, podemos monitorá-lo. Conseguimos observar ao acessar a aba de *Hosts* que esse agente está listado e com *Items/Triggers* e *Graphs* já configurados

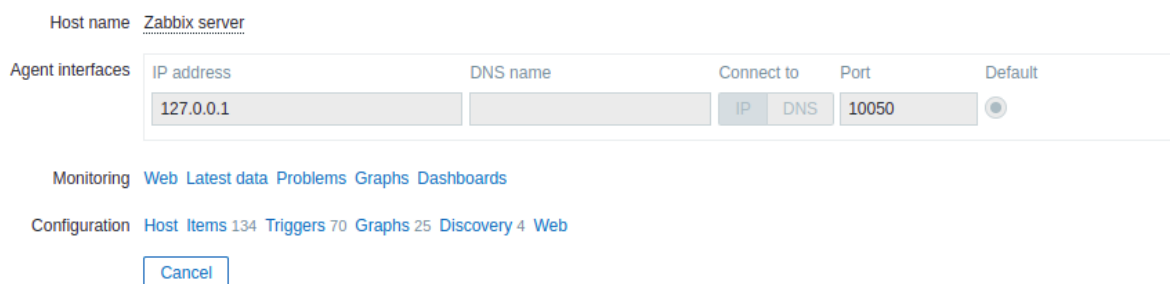


Figura 4. Configuração do Primeiro Agente (Notebook1).

Para fazer um teste inicial, vamos analisar a quantidade de bits que estão passando pela interface de rede *Wi-fi*. Na imagem abaixo, visualizamos o gráfico de *bits sent + bits received* da interface de rede *wlp0s20f3*. É possível visualizar um pico de banda, justificado pelo tráfego de teste de *upload* e *download* HTTP que eu executei na máquina enquanto os dados estavam sendo coletados.

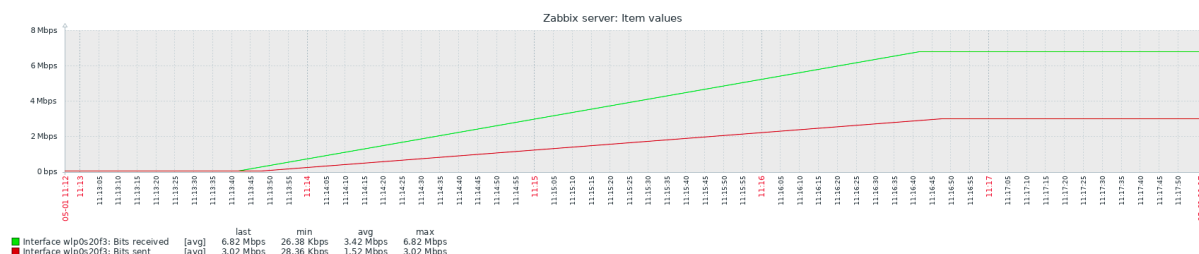


Figura 5. Gráfico mostrando *bits sent + bits received* da interface de rede do Notebook1.

Agora, que visualizamos que o *Zabbix* está coletando métricas corretamente, vamos instalar os processos agentes nas máquinas gerenciadas e fazer os testes com elas. Como estamos usando sistemas operacionais diferentes, no Windows, o processo é um pouco diferente. Todavia, em todas as máquinas basta instalar o Zabbix Agent, liberar o tráfego no firewall para a porta 10050, que é a porta que o Servidor Zabbix usa para conexão TCP. E depois, registrar o host no Zabbix. Na imagem abaixo vemos um exemplo de configuração para o sistema operacional Windows:

Host

Host IPMI Tags Macros Inventory Encryption Value mapping

* Host name Workstation

Visible name Workstation

Templates

Name	Action
Windows by Zabbix agent	Unlink Unlink and clear

type here to search

* Groups

Templates/Operating systems

type here to search

Interfaces

Type	IP address	DNS name	Connect to	Port	Default
Agent	192.168.178.231		IP DNS	10050	<input checked="" type="radio"/> Remove

[Add](#)

Description

Monitored by proxy (no proxy)

Enabled ☒

Figura 6. Configuração do Host Workstation no Zabbix.

Depois de configurar, podemos visualizar as métricas coletadas pelo gerente, nesse exemplo, estamos monitorando o tráfego na interface de rede do host Workstation, o host que hospeda o sistema operacional Windows.

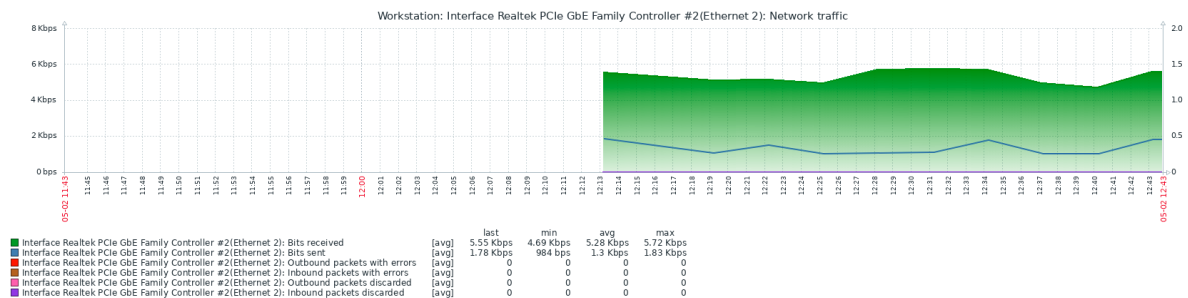


Figura 7. Gráfico do tráfego de rede do host Workstation.

Também devemos configurar o host Notebook2. Após liberar as portas no firewall e fazer a instalação do Zabbix Agent, configuramos o Notebook2 da seguinte maneira no Zabbix:

Host

Host IPMI Tags Macros Inventory Encryption Value mapping

* Host name

Visible name

Templates

Name	Action
Linux by Zabbix agent	Unlink Unlink and clear

* Groups

Interfaces

Type	IP address	DNS name	Connect to	Port	Default
Agent	<input type="text" value="192.168.178.211"/>	<input type="text"/>	<input checked="" type="radio"/> IP <input type="radio"/> DNS	<input type="text" value="10050"/>	<input checked="" type="radio"/> Remove

[Add](#)

Description

Monitored by proxy

Enabled ☒

Figura 8. Configuração do Host Notebook2.

Foi adicionado o template de **Linux by Zabbix Agent**, automatizando diversas configurações, como regras de descoberta e chaves de monitoramento. Depois de configurado, podemos visualizar as métricas, na imagem seguinte estamos monitorando o disk space usage (uso de disco) do host Notebook2:

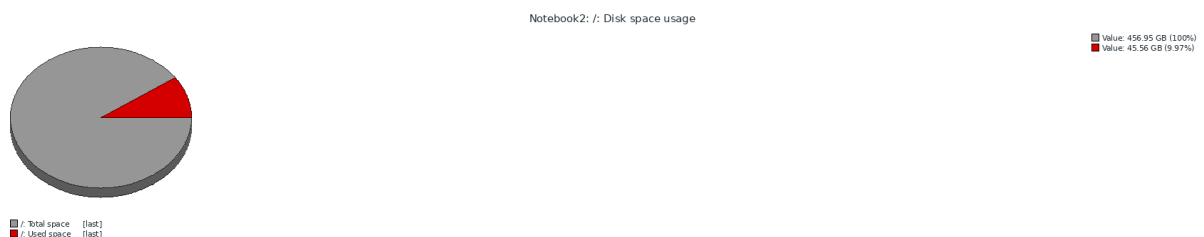


Figura 9. Espaço de Disco no Notebook2.

Teste de Wireshark para Notebook2.

Com o fim de visualizar a troca de pacotes entre o ambiente central e o host Notebook2 (192.168.178.211) e validar a troca de informações, usamos a ferramenta **Wireshark**, para capturar pacotes e filtramos pelo filtro “ip.addr == 192.168.178.211” que irá filtrar apenas pacotes que contém este endereço IP no cabeçalho. Buscamos o pacote que envia o número de processos para o Zabbix, o nome desse item é **Number of processes** e sua chave de monitoramento é **proc.num** do tipo Zabbix Agent. Na figura 10, conseguimos ver o servidor pedindo para o agente o número de processos através da chave proc.num, ao seguir o

fluxo TCP deste pacote, conseguimos encontrar o valor de resposta, que é

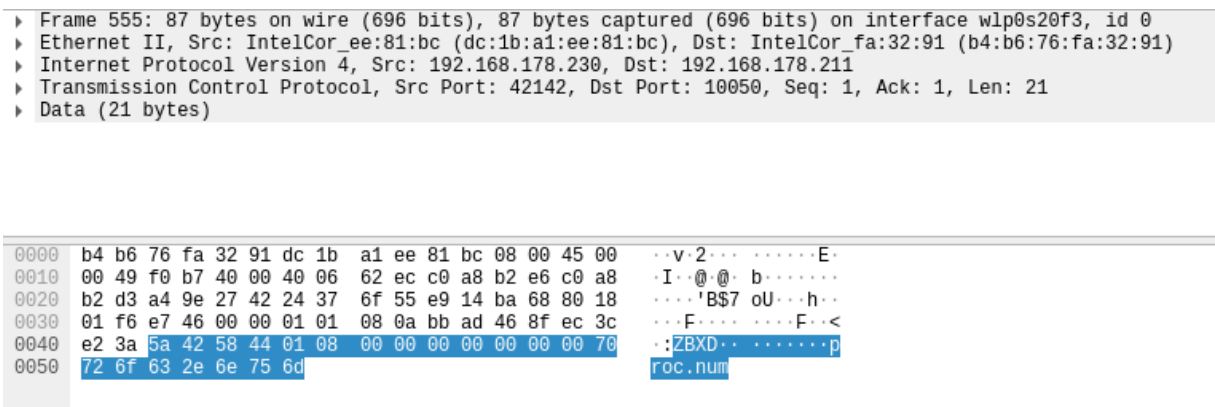


Figura 10. Requisição do Zabbix para número de processos no Notebook2.

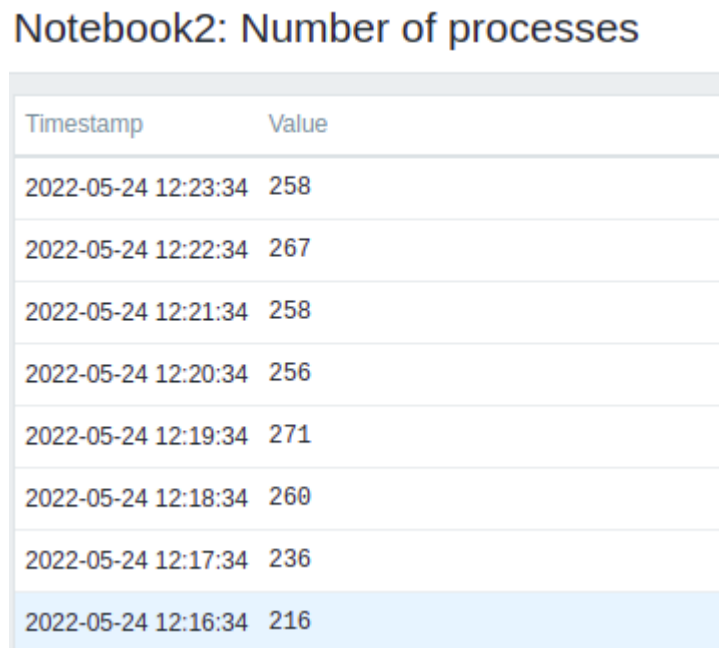


Figura 11. Últimos valores de número de processos no Notebook2 no Zabbix Server.

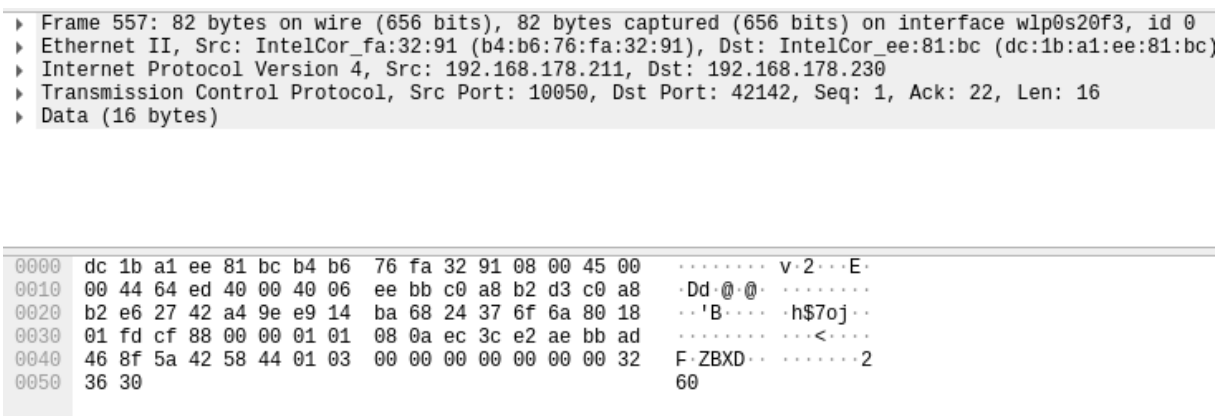


Figura 12. Pacote de resposta para requisição.

Podemos visualizar na Figura 12. O pacote que envia o número 260 e na Figura 11 o número de 260 expresso na interface de frontend do Zabbix, certificando-se de que o resultado foi inserido no backend da ferramenta e está sendo apresentado com sucesso. Após o envio do pacote, encerra-se a comunicação TCP através das flags [FIN ACK]; [FIN ACK]; [ACK].

5.1 Wireshark para gerência de redes

Para visualizar a troca de tráfego entre os Hosts, usamos a ferramenta **Wireshark**, uma ferramenta de captura de tráfego. Como o Zabbix Server usa o protocolo TCP para conectar com o Agente e trocar dados, vamos seguir uma TCP Stream para visualizar o tráfego entre o gerente e o agente. Nesse caso é a [tcp.stream 150](#), que está transmitindo o número de threads do host Workstation. Na Figura 13 podemos ver a captura desse tráfego.

tcp.stream eq 150						
No.	Time	Source	Destination	Protocol	Length	Info
6482	149.193715943	192.168.178.230	192.168.178.231	TCP	74	34592 → 10050 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK PERM=...
6488	149.204713369	192.168.178.231	192.168.178.230	TCP	62	10050 → 34592 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460...
6489	149.204722406	192.168.178.230	192.168.178.231	TCP	54	34592 → 10050 [ACK] Seq=1 Ack=1 Win=64240 Len=0
6491	149.204765400	192.168.178.230	192.168.178.231	TCP	101	34592 → 10050 [PSH, ACK] Seq=1 Ack=1 Win=64240 Len=47
6492	149.207145531	192.168.178.231	192.168.178.230	TCP	78	10050 → 34592 [PSH, ACK] Seq=1 Ack=48 Win=64193 Len=24
6493	149.207149483	192.168.178.230	192.168.178.231	TCP	54	34592 → 10050 [ACK] Seq=48 Ack=25 Win=64216 Len=0
6494	149.207195384	192.168.178.230	192.168.178.231	TCP	54	34592 → 10050 [FIN, ACK] Seq=48 Ack=25 Win=64216 Len=0
6495	149.207753271	192.168.178.231	192.168.178.230	TCP	60	10050 → 34592 [FIN, ACK] Seq=25 Ack=48 Win=64193 Len=0
6496	149.207756722	192.168.178.230	192.168.178.231	TCP	54	34592 → 10050 [ACK] Seq=49 Ack=26 Win=64215 Len=0
6502	149.419532876	192.168.178.230	192.168.178.231	TCP	54	[TCP Retransmission] 34592 → 10050 [FIN, ACK] Seq=48 Ack=26 W...
6503	149.423179460	192.168.178.231	192.168.178.230	TCP	60	[TCP ZeroWindow] 10050 → 34592 [ACK] Seq=26 Ack=49 Win=0 Len=0

Figura 13. TCP Stream entre Workstation e Notebook1 (Zabbix Server).

▶ Frame 6491: 101 bytes on wire (808 bits), 101 bytes captured (808 bits) on interface wlp0s20f3, id 0	
▶ Ethernet II, Src: IntelCor_ee:81:bc (dc:1b:a1:ee:81:bc), Dst: ASRockIn_f6:51:e1 (70:85:c2:f6:51:e1)	
▶ Internet Protocol Version 4, Src: 192.168.178.230, Dst: 192.168.178.231	
▶ Transmission Control Protocol, Src Port: 34592, Dst Port: 10050, Seq: 1, Ack: 1, Len: 47	
▼ Data (47 bytes)	
Data: 5a4258440122000000000000007065f72665f636f756e7465...	
[Length: 47]	
0000 70 85 c2 f6 51 e1 dc 1b a1 ee 81 bc 08 00 45 00 p...Q... ..E..	
0010 00 57 99 5a 40 00 40 06 ba 27 c0 a8 b2 e6 c0 a8 .W.Z@.@. .'.	
0020 b2 e7 87 20 27 42 d5 a1 81 ab 94 6b b1 2f 50 18 ...'B... ..k./P..	
0030 fa f0 e7 68 00 00 5a 42 58 44 01 22 00 00 00 00 ...h.ZB.XD..	
0040 00 00 00 70 65 72 66 5f 63 6f 75 6e 74 65 72 5f ...perf_counter...	
0050 65 6e 5b 22 5c 53 79 73 74 65 6d 5c 54 68 72 65 en["\System\Thre...	
0060 61 64 73 22 5d ads"]	

Figura 14. Cabeçalho de dados da requisição do gerente.

Basta olhar o cabeçalho de dados, na figura 14, que está sendo transmitido em texto claro entre o processo gerente e o processo agente, que visualizamos a chave que o processo gerente (192.168.178.230) está buscando no host 192.168.178.231 (Workstation). Na figura 15, visualizamos a configuração do item no Zabbix Server:

* Name	Number of threads
Type	Zabbix agent ▼
* Key	perf_counter_en["\System\Threads"]
Type of information	Numeric (unsigned) ▼
* Host interface	192.168.178.231:10050 ▼

Figura 15. Configuração do item requisitado no Zabbix.

Na figura 16, visualizamos a resposta do agente e temos o número de 1294 threads.

```

▶ Frame 6492: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface wlp0s20f3, id 0
▶ Ethernet II, Src: ASRockIn_f6:51:e1 (70:85:c2:f6:51:e1), Dst: IntelCor_ee:81:bc (dc:1b:a1:ee:81:bc)
▶ Internet Protocol Version 4, Src: 192.168.178.231, Dst: 192.168.178.230
▶ Transmission Control Protocol, Src Port: 10050, Dst Port: 34592, Seq: 1, Ack: 48, Len: 24
▼ Data (24 bytes)
  Data: 5a425844010b00000000000000313239342e303030303030
  [Length: 24]

```


0000	dc 1b a1 ee 81 bc 70 85 c2 f6 51 e1 08 00 45 00p. .Q. .E.
0010	00 40 d9 9c 40 00 80 06 39 fc c0 a8 b2 e7 c0 a8	..@..@.. 9.....
0020	b2 e6 27 42 87 20 94 6b b1 2f d5 a1 81 da 50 18	.. 'B. .k . / . . . P.
0030	fa c1 d7 9e 00 00 5a 42 58 44 01 0b 00 00 00 00ZB XD.....
0040	00 00 00 31 32 39 34 2e 30 30 30 30 30 30 30 30	...1294. 000000

Figura 16. Cabeçalho de dados da resposta do agente para a requisição feita.

6. QUESTIONÁRIO DE SATISFAÇÃO DOS USUÁRIOS

O seguinte questionário foi realizado com os usuários da rede para levantar dados em relação aos serviços prestados pela rede:

Pergunta 1. Como você classificaria o desempenho geral da rede?

Pergunta 2. O quão estável é a rede? E a disponibilidade dos serviços?

Pergunta 3. Classifique em relação ao tempo gasto para que o suporte técnico resolva eventuais problemas.

Pergunta 4. Como é a qualidade dos serviços providos pelo suporte técnico?

Pergunta 5. Como é a qualidade do acesso à rede externa (Internet)?

Pergunta 6. Como é a qualidade dos serviços prestados?

Pergunta 7. Como é a qualidade da segurança da rede?

6.1. Como você classificaria o desempenho geral da rede?

Para a primeira pergunta, em relação ao desempenho geral da rede, a maioria dos usuários considera Bom ou Ótimo, sendo que uma grande parcela, cerca de 34,3% dos usuários consideram ruim.

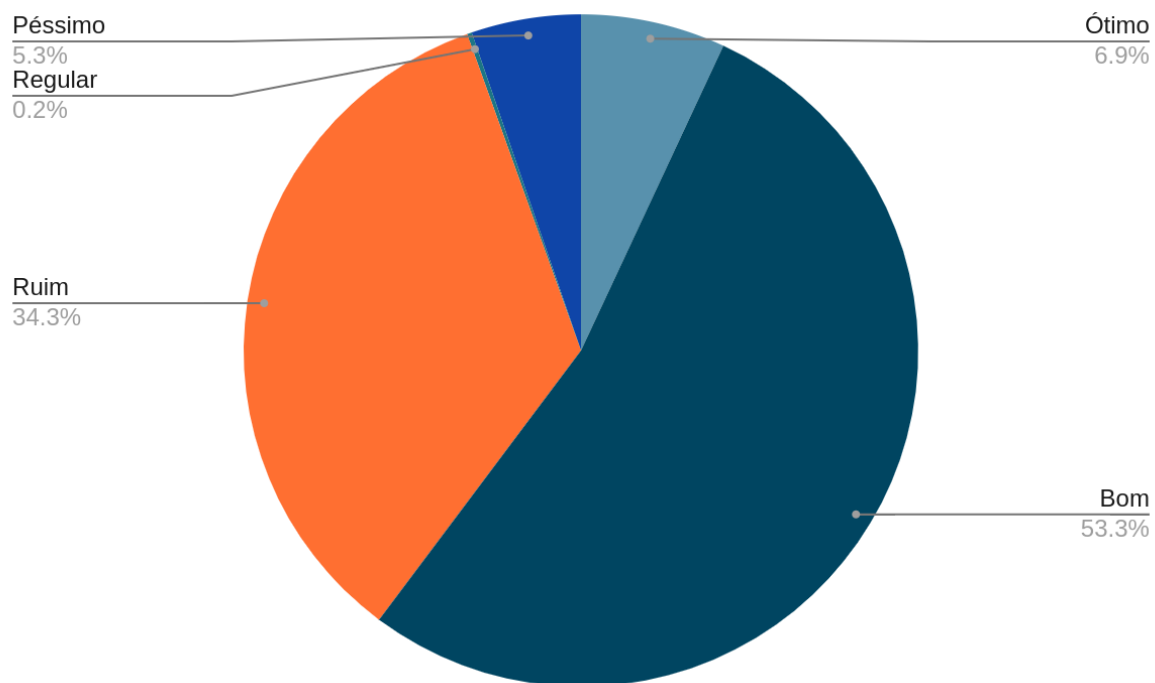


Figura 17. Gráfico da distribuição de respostas do questionário para a pergunta 1.

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

Para a segunda pergunta, em relação a disponibilidade dos serviços da rede, a maioria dos usuários considera Péssimo ou Regular, ou seja, a rede se apresenta muito instável, gerando insatisfação para os usuários.

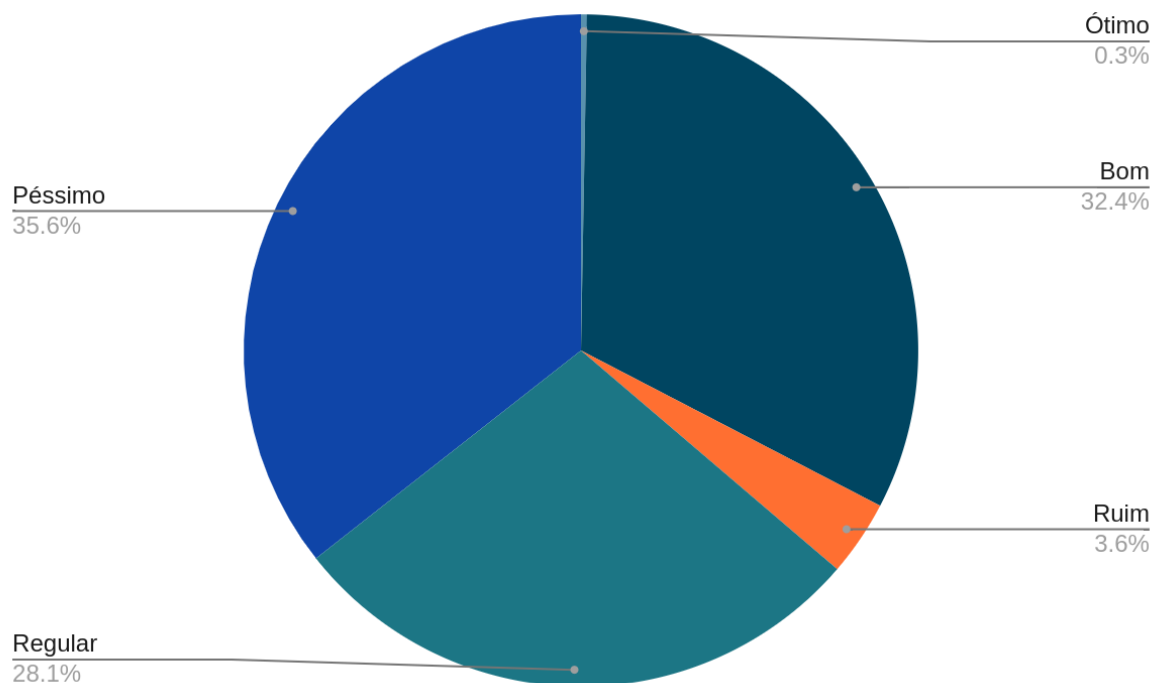


Figura 18. Gráfico da distribuição de respostas do questionário para a pergunta 3.

6.3. Classifique em relação ao tempo gasto para que o suporte técnico resolva eventuais problemas

Sobre os resultados da terceira pergunta, em relação ao tempo gasto para que o suporte técnico resolva eventuais problemas, a maioria dos usuários considera Péssimo ou Ótimo, ou seja, as opiniões estão bem divididas. Todavia, significa que o time técnico deve aprimorar o seu atendimento, devido ao alto número de usuários insatisfeitos

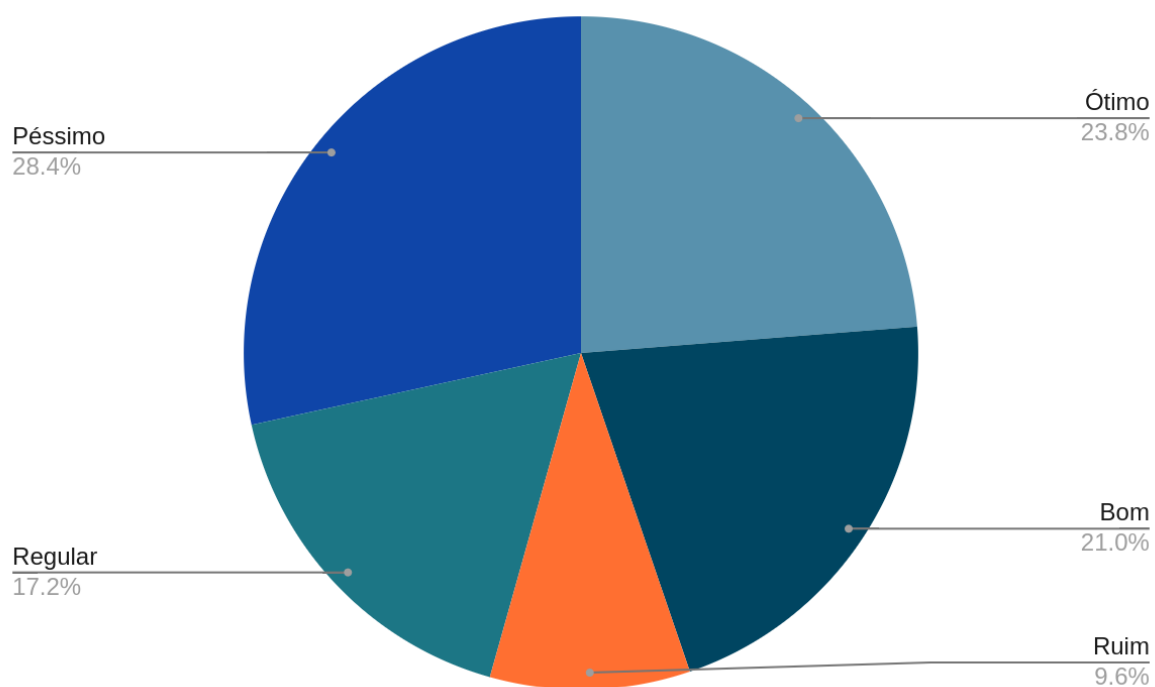


Figura 19. Gráfico da distribuição de respostas do questionário para a classificação 3.

6.4. Como é a qualidade dos serviços providos pelo suporte técnico?

Sobre os resultados da quarta pergunta, em relação a qualidade dos serviços providos pelo suporte técnico. Cerca de 35% consideram Péssimo, e cerca de 17% consideram ruim, ou seja, a maioria dos usuários estão insatisfeitos com os serviços providos pelo suporte técnico. Indicando um ponto de melhoria.

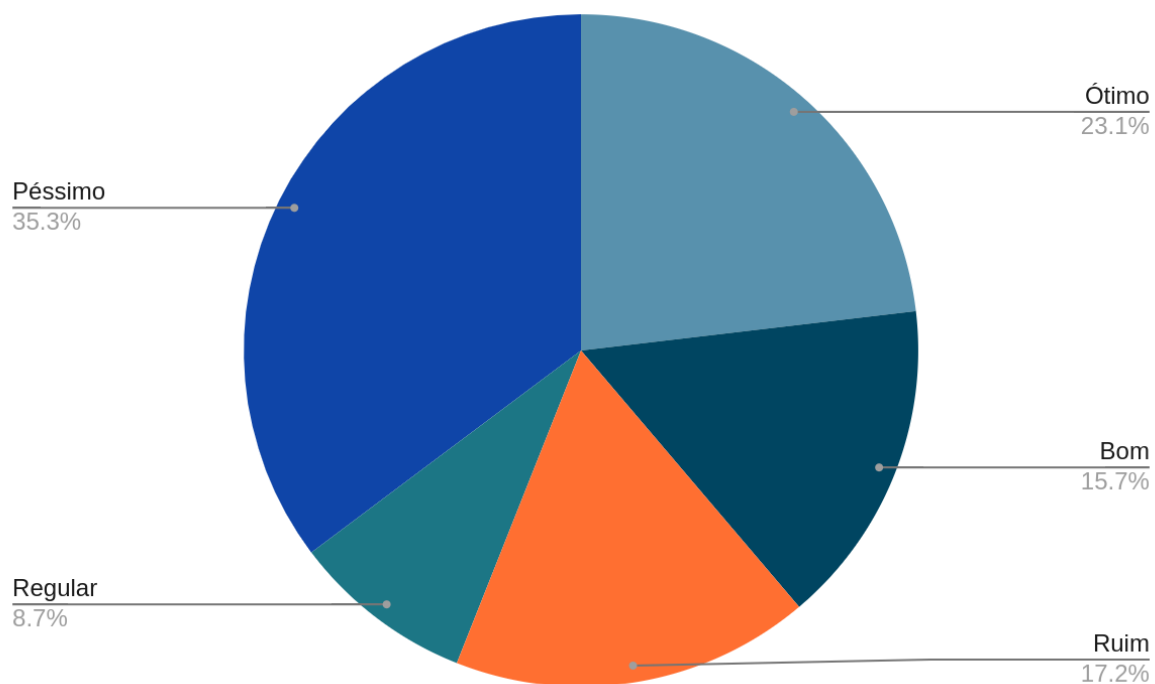


Figura 20. Gráfico da distribuição de respostas do questionário para a pergunta 4.

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

Sobre os resultados da quinta pergunta, em relação a qualidade de acesso à rede externa. A maioria dos usuários consideram ou ótimo, ou bom ou regular. E, cerca de 22% acreditam que a qualidade é ruim. Indicando um ponto de melhoria.

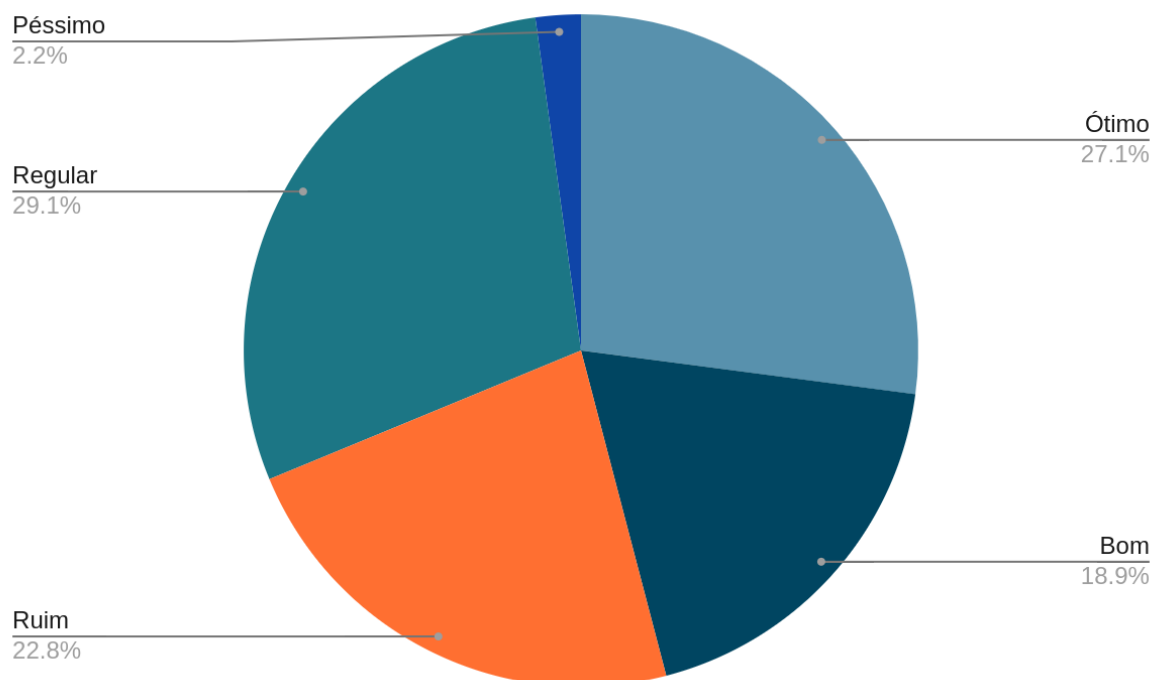


Figura 21. Gráfico da distribuição de respostas do questionário para a pergunta 5.

6.6. Como é a qualidade dos serviços prestados?

Sobre os resultados da sexta pergunta, em relação a qualidade dos serviços prestados. A grande maioria dos usuários acha Ruim. Sendo que apenas 2.9% consideram ótimo e 6.5% consideram bom, indicando que a qualidade dos serviços prestados deve aprimorada com urgência.

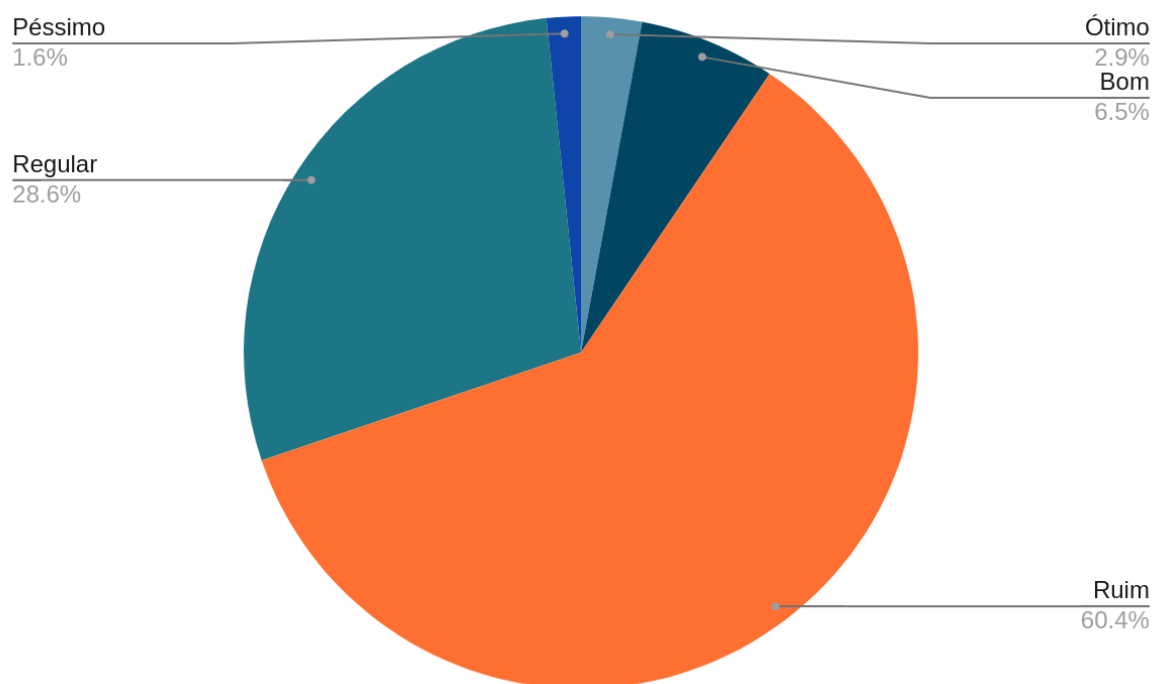


Figura 22. Gráfico da distribuição de respostas do questionário para a pergunta 6.

6.7. Como é a qualidade da segurança da rede?

Para a sétima pergunta, em relação a qualidade da segurança da rede. A maioria dos usuários considera ou ótimo, ou bom. Sendo que 24% consideram regular e cerca de 24% consideram Ruim ou péssimo. Ou seja, há possibilidade de melhorar a segurança da rede.

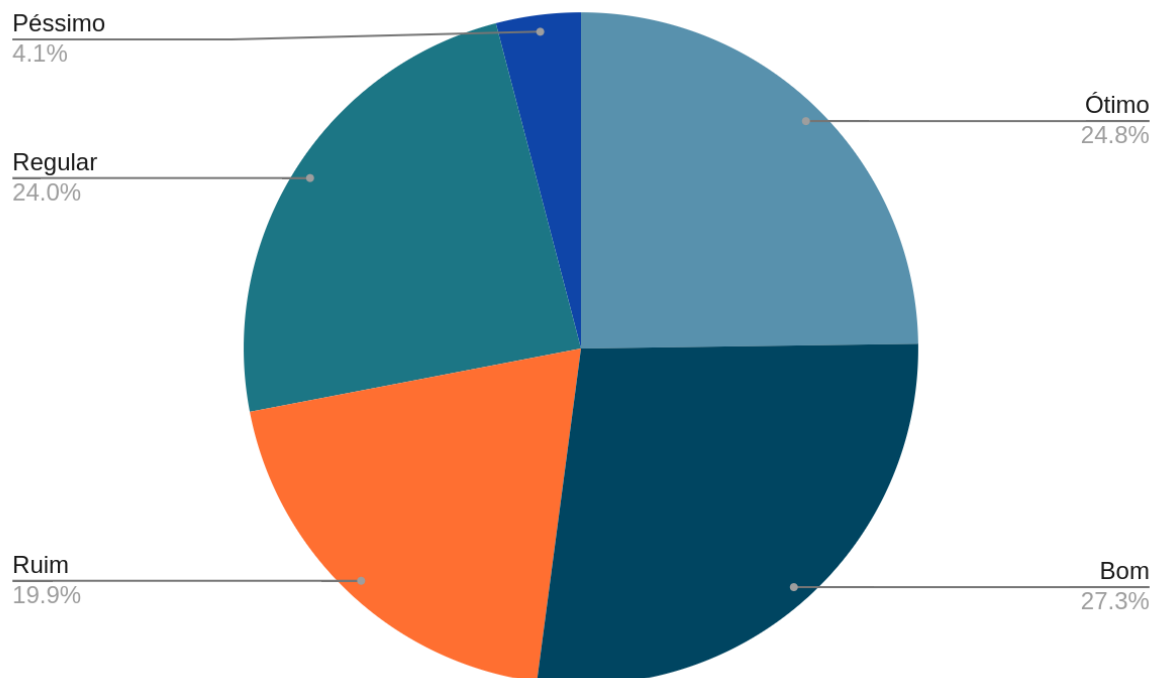


Figura 23. Gráfico da distribuição de respostas do questionário para a pergunta 7.

7. ACORDO DE NÍVEL DE SERVIÇO - SLA

CONTRATO DE ACORDO DE NÍVEL DE SERVIÇO

7.1 Visão Geral

Cláusula 1. Este contrato tem o fim de definir um Acordo de Nível de Serviço entre a parte contratada e a parte contratante. Todas as cláusulas deverão ser seguidas e respeitadas. Em caso de desrespeito às cláusulas, as partes do contrato estão sujeitas à penalidades.

Cláusula 2. Esse contrato tem validade de 24 meses, a partir da data de início efetivo definida ao final do contrato.

Cláusula 3. Este acordo define os serviços prestados pela parte contratada, junto das métricas requisitadas e que devem ser respeitadas para manter o nível de qualidade que a parte contratante está solicitando. Em caso de desrespeito, este acordo prevê multas à parte contratada.

7.2 Sumário Executivo

Cláusula 4. Fica estabelecido que o responsável por prover os serviços de gerência e administração de redes será o provedor de serviço(s) “CONTRATADO”, doravante denominado “contratado” ou “provedor”.

Cláusula 5. Fica estabelecido que o cliente será “CONTRATANTE”, doravante denominado “contratante” ou “cliente”.

Cláusula 6. O presente Contrato de Acordo de Nível de Serviço tem como objetivo garantir à parte contratante os compromissos e elementos definidos neste contrato pela parte contratada. Com o fim de prover a entrega constante de informações relacionadas aos serviços prestados ao contratante. Os serviços definidos neste contrato são:

- Segurança;
- Disponibilidade de recursos definidos na rede;
- Administração e Gerência dos recursos da rede;
- Transparência;
- Suporte técnico em reparos e manutenções.

Cláusula 7. Horários do Centro de Operações de Rede - O provedor de serviço possui um centro de operações de rede, podendo ser referido como NOC (*Network Operations Center*). O suporte técnico provido pela equipe de operações abrange os seguintes horários

- das 7h às 23h em dias úteis
- das 8h às 20h em fins de semana e feriados.

O time de operações pode ser acionado a qualquer momento no horário definido acima na pelos seguintes meios:

- Telefone: +55 (48) 3333-3333
- E-mail: noc@exemplo-sla.br

Cláusula 8. Em caso de necessidade de reparos emergenciais, definidos como prioridade máxima, o contrato obriga ao contratado o reparo em até 12 horas corridas a partir da abertura do chamado de reparo com o time de operação, A situação será avaliada posteriormente pelo comitê gestor, e caso o acordo desta cláusula seja rompido, o contrato prevê multa de 5.500 R\$ para o contratado.

Cláusula 9. O provedor de serviço deverá notificar o cliente via e-mail cadastrado no sistema do contratado, sobre todas as operações de manutenção agendadas que possam vir a causar alguma indisponibilidade ou impacto no desempenho da rede.

Cláusula 10. Relatórios Periódicos - O provedor de serviço deverá realizar medições mensais da rede e enviar relatórios de disponibilidade para o cliente, com o fim de avaliar o desempenho da rede. Os relatórios mensais devem conter:

- Estatísticas de disponibilidade dos recursos de rede;
- Estatísticas de recursos alocados para o cliente, caso existam;
- Manutenções programadas no mês;

7.3 Parâmetros e Métricas de Desempenho do Serviço Contratado

Cláusula 11. Reserva-se um intervalo de 3 (três) horas para manutenção e reparos da rede em horários de pouco ou nenhum tráfego, mediante aviso prévio ao cliente.

Cláusula 12. O acesso à rede externa deve ter 100% de disponibilidade, ou seja, o centro de processamento de dados responsável por levar o tráfego ao *backbone* da internet deve sempre estar disponível pela rota principal ou enlaces alternativos.

7.4 Escopo de Serviço

Cláusula 13. Os seguintes itens e níveis devem ser respeitados:

1. O número de Threads em Workstations não deve ultrapassar 2000.
2. A utilização da memória host Workstation não pode ultrapassar 90%.
3. A taxa de transferência da interface de rede do Notebook2 não deve ultrapassar 10Mbps de download e/ou upload.
4. O host gerente não pode ter o uptime zerado durante o tempo monitorado.
5. O número de Inodes disponível no host gerente não pode ser menor que 90%.
6. O número de conexões ativas na porta 443 do host Notebook2 não pode ser maior que 10.

7.5 Sanções e Penalidades

Cláusula 14. Esta cláusula define as sanções e penalidades aplicadas ao contratado em caso da configuração de quebra do escopo de serviço.

- ❖ Em caso de quebra de qualquer cláusula, o responsável pela quebra, deverá pagar uma multa de 1.000 R\$ para a parte afetada.
- ❖ Em caso de desrespeito ao Item 2 da Cláusula 13, a parte contratada deverá liquidar o valor de 18.750 R\$ para o cliente.
- ❖ Em caso de quebra de 2 (duas) ou mais cláusulas, o contratante terá direito a revisão do contrato e caso tenha passado o período de pelo menos 12 (doze) meses a partir da data de início efetivo do acordo, o cliente terá o direito de rescisão do contrato.

7.6 Responsabilidades Mútuas

Cláusula 15. Este acordo tem validade a partir da data efetiva definida abaixo. Ao término do contrato ou após o período de 12 (doze) meses, é necessário uma revisão pela parte contratada e parte contratante.

Cláusula 16. A revisão do contrato se dará por uma reunião em que ambas partes irão decidir se o contrato será renovado no próximo período de exercício contratual. Após a decisão, ambas partes tem o período de 30 dias para realizar uma submissão formal com o fim de alterar alguma cláusula.

Cláusula 17. Será responsabilidade do provedor dos serviços cumprir com os serviços e garantias precisados no contrato presente, encarregando-se de cobrir os horários e respeitar as métricas definidas.

Cláusula 18. Será responsabilidade do cliente concernir o acordo presente e os termos acordados por ambas as partes, respeitando sua cobertura de horários. Será também responsabilidade do contratante não suprimir informações demandadas provenientes do uso de algum serviço prestado pela parte contratada, além de liquidar o valor mensal de 3.500 R\$ para a parte contratada.

Contratante (Cliente)

Testemunha

Contratado (Provedor)

Testemunha

Data de Início Efetivo

8. ACORDO DE NÍVEL DE SERVIÇO EM UML

O diagrama UML abaixo representa o contrato SLA, temos no centro a classe *SLA*, que contém um contratado do tipo *PessoaJuridica* e um contratante do tipo *PessoaJuridica*, além da data de início efetivo do contrato e um conjunto de cláusulas. A classe *PessoaJuridica* possui duas relações de **agregação** 1 para 1 com a classe *SLA*, uma sendo para o contratante e outra sendo para o contratado. Uma instância de *PessoaJuridica* irá conter uma razão social, um CNPJ e uma breve descrição das atividades da Pessoa Jurídica. A classe *Clausula*, possui um identificador, uma descrição e uma métrica, e possui uma relação de agregação com o contrato *SLA*, um contrato *SLA* pode ter 1 ou mais cláusulas e uma cláusula contém apenas 1 contrato. A Cláusula possui uma métrica e a métrica possui uma medição. O Objeto *Metrica* contém um nome, uma descrição, uma restrição e uma medição. O objeto *Medicao* possui uma data de início, uma data de término e uma coleção de valores inteiros.

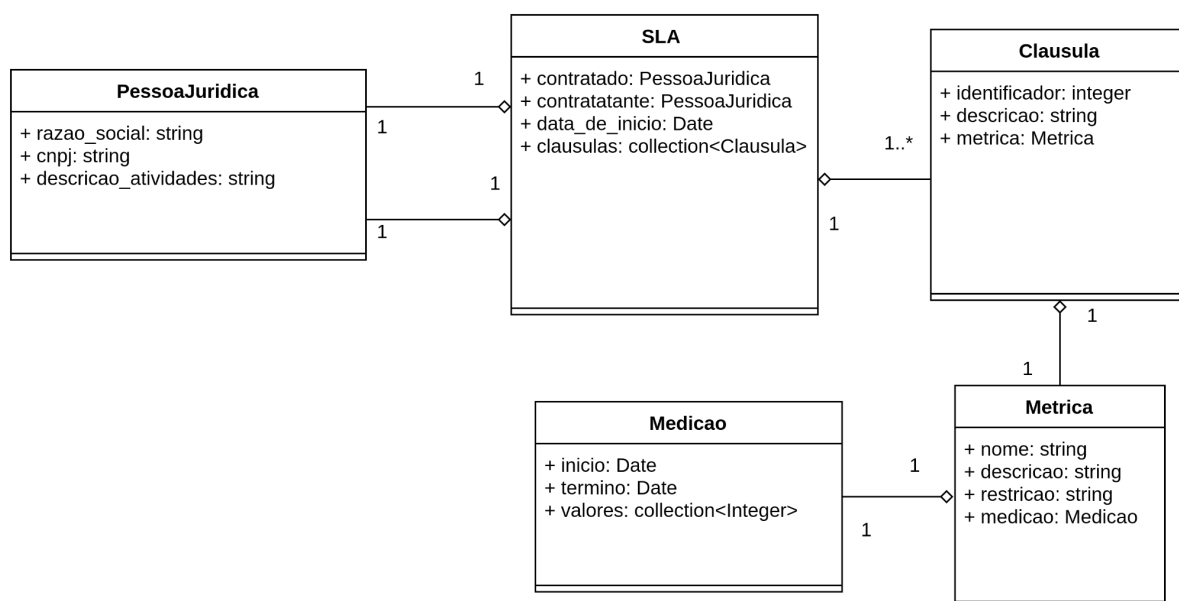


Figura 24. Diagrama em UML.

9. ACORDO DE NÍVEL DE SERVIÇO EM XML

Nesta seção temos a definição do SLA em XML (eXtensible Markup Language), ou seja, o SLA especificado em uma linguagem de marcação caso seja necessário o compartilhamento dessa informação via internet de maneira adequada e recomendada pela W3C. O contrato está com a codificação em UTF-8, usando a versão XML 1.0, as **tags** estão escritas de um modo que seja intuitivo a descoberta dos dados, ou seja, o título do SLA, está dentro da tag **title**, as cláusulas estão inseridas junto de sua numeração nas tags **clause**, e as tags **clause**, contém tags **description**, que contém a descrição da cláusula. O bloco de código abaixo descreve o contrato na linguagem XML:

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<sla>
  <title>
    CONTRATO DE ACORDO DE NIVEL DE SERVICO
  </title>
  <section>
    6.1 Visão Geral
    <clause>
      Cláusula 1.
      <description>
        Este contrato tem o fim de definir um Acordo de Nível
de Serviço entre a parte contratada e a parte contratante. Todas as
cláusulas deverão ser seguidas e respeitadas. Em caso de desrespeito
às cláusulas, as partes do contrato estão sujeitas à penalidades.
      </description>
    </clause>
    <clause>
      Cláusula 2.
      <description>
        Esse contrato tem validade de 24 meses, a partir da
data de início efetivo definida ao final do contrato.
      </description>
    </clause>
    <clause>
      Cláusula 3.
      <description>
        Este acordo define os serviços prestados pela parte
contratada, junto das métricas requisitadas e que devem ser
respeitadas para manter o nível de qualidade que a parte contratante
está solicitando. Em caso de desrespeito, este acordo prevê multas à
parte contratada.
      </description>
    </clause>
  </section>
  <section>
    6.2 Sumário Executivo
    <clause>
      Cláusula 4.
      <description>
        Fica estabelecido que o responsável por prover os
serviços de gerência e administração de redes será o provedor de

```

```

serviço(s) "CONTRATADO", doravante denominado "contratado" ou
"provedor".
    </description>
</clause>
<clause>
    Cláusula 5.
    <description>
        Fica estabelecido que o cliente será "CONTRATANTE",
        doravante denominado "contratante" ou "cliente".
    </description>
</clause>
<clause>
    Cláusula 6.
    <description>
        O presente Contrato de Acordo de Nível de Serviço tem
        como objetivo garantir à parte contratante os compromissos e elementos
        definidos neste contrato pela parte contratada. Com o fim de prover a
        entrega constante de informações relacionadas aos serviços prestados
        ao contratante. Os serviços definidos neste contrato são:
        <description_item>
            Segurança;
        </description_item>
        <description_item>
            Disponibilidade de recursos definidos na rede;
        </description_item>
        <description_item>
            Administração e Gerência dos recursos da rede;
        </description_item>
        <description_item>
            Transparência;
        </description_item>
        <description_item>
            Suporte técnico em reparos e manutenções.
        </description_item>
    </description>
</clause>
<clause>
    Cláusula 7.
    <description>
        Horários do Centro de Operações de Rede - O provedor de
        serviço possui um centro de operações de rede, podendo ser referido
        como NOC (Network Operations Center). O suporte técnico provido pela

```

equipe de operações abrange os seguintes horários

```
<description_item>
```

das 7h às 23h em dias úteis

```
</description_item>
```

```
<description_item>
```

das 8h às 20h em fins de semana e feriados.

```
</description_item>
```

O time de operações pode ser acionado a qualquer momento no horário definido acima na pelos seguintes meios:

```
<description_item>
```

Telefone: +55 (48) 3333-3333

```
</description_item>
```

```
<description_item>
```

E-mail: noc@exemplo-sla.br

```
</description_item>
```

```
</description>
```

```
</clause>
```

```
<clause>
```

Cláusula 8.

```
<description>
```

Em caso de necessidade de reparos emergenciais, definidos como prioridade máxima, o contrato obriga ao contratado o reparo em até 12 horas corridas a partir da abertura do chamado de reparo com o time de operação, A situação será avaliada posteriormente pelo comitê gestor, e caso o acordo desta cláusula seja rompido, o contrato prevê multa de 5.500 R\$ para o contratado.

```
</description>
```

```
</clause>
```

```
<clause>
```

Cláusula 9.

```
<description>
```

O provedor de serviço deverá notificar o cliente via e-mail cadastrado no sistema do contratado, sobre todas as operações de manutenção agendadas que possam vir a causar alguma indisponibilidade ou impacto no desempenho da rede.

```
</description>
```

```
</clause>
```

```
<clause>
```

Cláusula 10.

```
<description>
```

Relatórios Periódicos - O provedor de serviço deverá realizar medições mensais da rede e enviar relatórios de

disponibilidade para o cliente, com o fim de avaliar o desempenho da rede. Os relatórios mensais devem conter:

```
<description_item>
    Estatísticas de disponibilidade dos recursos de
rede;
</description_item>
<description_item>
    Estatísticas de recursos alocados para o cliente,
caso existam;
</description_item>
<description_item>
    Manutenções programadas no mês;
</description_item>
</description>
</clause>
</section>
<section>
    6.3 Parâmetros e Métricas de Desempenho do Serviço Contratado
    <clause>
        Cláusula 11.
        <description>
            Reserva-se um intervalo de 3 (três) horas para
manutenção e reparos da rede em horários de pouco ou nenhum tráfego,
mediante aviso prévio ao cliente.
        </description>
    </clause>
    <clause>
        Cláusula 12.
        <description>
            O acesso à rede externa deve ter 100% de
disponibilidade, ou seja, o centro de processamento de dados
responsável por levar o tráfego ao backbone da internet deve sempre
estar disponível pela rota principal ou enlaces alternativos.
        </description>
    </clause>
</section>
<section>
    6.4 Escopo de Serviço
    <clause>
        Cláusula 13.
        <description>
            Os seguintes itens e níveis devem ser respeitados:
```

```

        <description_item>
            O número de Threads em Workstations não deve
ultrapassar 2000.
        </description_item>
        <description_item>
            A interface de rede do host Workstation deve sempre
estar operacional.
        </description_item>
        <description_item>
            A interface de rede do host Workstation deve sempre
estar operacional.
        </description_item>
        <description_item>
            O host gerente não pode ter o uptime zerado durante
o tempo monitorado
        </description_item>
        <description_item>
            O número de Inodes disponível não pode ser menor
que 90%
        </description_item>
<description_item>O número de conexões ativas na porta 443 do host
Notebook2 não pode ser maior que 10.</description_item>
    </description>
</clause>
</section>
<section>
    6.5 Sanções e Penalidades
    <clause>
        Cláusula 14.
        <description>
            Esta cláusula define as sanções e penalidades aplicadas
ao contratado em caso da configuração de quebra do escopo de serviço.
        <description_item>
            Em caso de quebra de qualquer cláusula, o
responsável pela quebra, deverá pagar uma multa de 1.000 R$ para a
parte afetada.
        </description_item>
        <description_item>
            Em caso de desrespeito ao Item 2 da Cláusula 13. a
parte contratada deverá liquidar o valor de 18.750 R$ para o cliente.
        </description_item>
        <description_item>

```

Em caso de quebra de 2 (duas) ou mais cláusulas, o contratante terá direito a revisão do contrato e caso tenha passado o período de pelo menos 12 (doze) meses a partir da data de início efetivo do acordo, o cliente terá o direito de rescisão do contrato.

</description_item>

</description>

</clause>

</section>

<section>

6.6 Responsabilidades Mútuas

<clause>

Cláusula 15.

<description>

Este acordo tem validade a partir da data efetiva definida abaixo. Ao término do contrato ou após o período de 12 (doze) meses, é necessário uma revisão pela parte contratada e parte contratante.

</description>

</clause>

<clause>

Cláusula 16.

<description>

A revisão do contrato se dará por uma reunião em que ambas partes irão decidir se o contrato será renovado no próximo período de exercício contratual. Após a decisão, ambas partes tem o período de 30 dias para realizar uma submissão formal com o fim de alterar alguma cláusula.

</description>

</clause>

<clause>

Cláusula 17.

<description>

Será responsabilidade do provedor dos serviços cumprir com os serviços e garantias precisados no contrato presente, encarregando-se de cobrir os horários e respeitar as métricas definidas.

</description>

</clause>

<clause>

Cláusula 18.

<description>

Este acordo define os serviços prestados pela parte

contratada, junto das métricas requisitadas e que devem ser respeitadas para manter o nível de qualidade que a parte contratante está solicitando. Em caso de desrespeito, este acordo prevê multas à parte contratada.

```
        </description>
    </clause>
</section>
<signatures>
    <date>
        data de início efetivo
    </date>
    <sign_contratante>
        Contratante
    </sign_contratante>
    <sign_contratado>
        Contratado
    </sign_contratado>
    <sign_testemunha>
        Testemunha
    </sign_testemunha>
    <sign_testemunha>
        Testemunha
    </sign_testemunha>
</signatures>
</sla>
```

Bloco de Código 1. Contrato SLA em XML.

10. VALIDAÇÃO DO XML

O bloco de código abaixo é o XML Schema usado para validar o contrato em XML definido na seção 8 pelo bloco de código 1. Um XML Schema é uma descrição de um tipo de documento XML, geralmente expressando em termos de restrições sobre a estrutura do documento. Essas restrições são expressadas usando combinações de regras gramaticais que conduzem a ordem dos elementos.

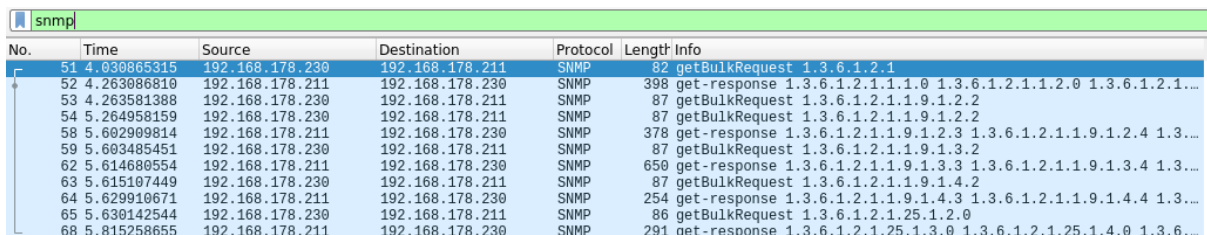
```
<xs:schema attributeFormDefault="unqualified"
elementFormDefault="qualified"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
    <xs:element name="sla">
        <xs:complexType>
            <xs:sequence>
                <xs:element type="xs:string" name="title"/>
                <xs:element name="section" maxOccurs="unbounded"
minOccurs="0">
                    <xs:complexType mixed="true">
                        <xs:sequence>
```

```
<xs:element name="clause" maxOccurs="unbounded"
minOccurs="0">
  <xs:complexType mixed="true">
    <xs:sequence>
      <xs:element name="description">
        <xs:complexType mixed="true">
          <xs:sequence>
            <xs:element type="xs:string"
name="description_item" maxOccurs="unbounded" minOccurs="0"/>
          </xs:sequence>
        </xs:complexType>
      </xs:element>
    </xs:sequence>
  </xs:complexType>
</xs:element>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name="signatures">
  <xs:complexType>
    <xs:sequence>
      <xs:element type="xs:string" name="date"/>
      <xs:element type="xs:string" name="sign_contratante"/>
      <xs:element type="xs:string" name="sign_contratado"/>
      <xs:element type="xs:string" name="sign_testemunha"
maxOccurs="unbounded" minOccurs="0"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>
</xs:sequence>
</xs:complexType>
</xs:element>
</xs:schema>
```

Bloco de Código 2. XML Schema usado para validar o contrato SLA.

11. CONFIGURAÇÕES ADICIONAIS PARA *SNMP*

Vamos monitorar o host Notebook2 com o protocolo *SNMP* além do Zabbix Agent, para isso devemos instalar e configurar o *SNMP*. Então, precisamos instalar o pacote *snmpd* no agente e configurar em `/etc/snmp/snmpd.conf` o valor de *agentaddress* para “agentAddress udp:161,udp6:[::1]:161”. Permitindo tráfego *SNMP* IPv4 e IPv6. Além disso, é necessário liberar as portas no *firewall* através do comando “sudo ufw allow from 192.168.178.230 to any port 161”. Agora para validar que o tráfego *SNMP* está funcionando, executamos no host gerente o comando “snmpbulkwalk -v2c -c public 192.168.178.211” enquanto capturamos tráfego no *Wireshark*. Na figura 25 podemos visualizar o tráfego *SNMP* entre o processo agente (192.168.178.211) e gerente (192.168.178.230). Depois de configurar o suporte de interfaces de comunicação *SNMP* via porta 161 no Zabbix e cadastrar itens de monitoramentos *SNMP*, nesse caso, foi configurado para obter a cada 30 segundos o uptime do Notebook2. Com isso, na aba hosts, o ícone do host configurado deve ficar com o *SNMP* em verde, conforme a figura 26, esse ícone indica que existe um processo agente *SNMP* respondendo no host.



No.	Time	Source	Destination	Protocol	Length	Info
51	4.030865315	192.168.178.230	192.168.178.211	SNMP	82	getBulkRequest 1.3.6.1.2.1
52	4.263086810	192.168.178.211	192.168.178.230	SNMP	398	get-response 1.3.6.1.2.1.1.1.0 1.3.6.1.2.1.1.2.0 1.3.6.1.2.1...
53	4.263581388	192.168.178.230	192.168.178.211	SNMP	87	getBulkRequest 1.3.6.1.2.1.1.9.1.2.2
54	5.264958159	192.168.178.230	192.168.178.211	SNMP	87	getBulkRequest 1.3.6.1.2.1.1.9.1.2.2
58	5.602909814	192.168.178.211	192.168.178.230	SNMP	378	get-response 1.3.6.1.2.1.1.9.1.2.3 1.3.6.1.2.1.1.9.1.2.4 1.3...
59	5.603485451	192.168.178.230	192.168.178.211	SNMP	87	getBulkRequest 1.3.6.1.2.1.1.9.1.3.2
62	5.614680554	192.168.178.211	192.168.178.230	SNMP	658	get-response 1.3.6.1.2.1.1.9.1.3.3 1.3.6.1.2.1.1.9.1.3.4 1.3...
63	5.615107449	192.168.178.230	192.168.178.211	SNMP	87	getBulkRequest 1.3.6.1.2.1.1.9.1.4.2
64	5.629910671	192.168.178.211	192.168.178.230	SNMP	254	get-response 1.3.6.1.2.1.1.9.1.4.3 1.3.6.1.2.1.1.9.1.4.4 1.3...
65	5.630142544	192.168.178.230	192.168.178.211	SNMP	86	getBulkRequest 1.3.6.1.2.1.25.1.2.0
68	5.815258655	192.168.178.211	192.168.178.230	SNMP	291	get-response 1.3.6.1.2.1.25.1.3.0 1.3.6.1.2.1.25.1.4.0 1.3.6...

Figura 25. Tráfego *SNMP*.

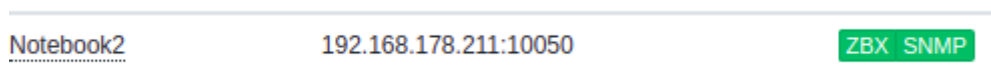


Figura 26. Configuração do *SNMP* no Zabbix.

12. EXTENSÃO DA MIB-2 *SNMP*

A extensão da MIB é usada para criar novos objetos gerenciáveis que podem ser tratados a partir do protocolo *SNMP*. Para estender a MIB, iremos usar um script para buscar o número de conexões ativas na porta 443 e criar um objeto gerenciável para esse dado. Então, primeiramente, criamos o script que irá fazer essa automação, usando o comando:

12.1. Criando o novo objeto e configurando o *SNMP*

```
caetano@ibm4381 ~$ vi con-port-443.sh
```

Ao executar o comando abrimos o editor de texto e escrevemos o script:


```

NET-SNMP-EXTEND-MIB::nsExtendArgs."443connections" = STRING:
/usr/bin/con-port-443.sh
NET-SNMP-EXTEND-MIB::nsExtendInput."443connections" = STRING:
NET-SNMP-EXTEND-MIB::nsExtendCacheTime."443connections" =
INTEGER: 5
NET-SNMP-EXTEND-MIB::nsExtendExecType."443connections" = INTEGER:
exec(1)
NET-SNMP-EXTEND-MIB::nsExtendRunType."443connections" = INTEGER:
run-on-read(1)
NET-SNMP-EXTEND-MIB::nsExtendStorage."443connections" = INTEGER:
permanent(4)
NET-SNMP-EXTEND-MIB::nsExtendStatus."443connections" = INTEGER:
active(1)
NET-SNMP-EXTEND-MIB::nsExtendOutput1Line."443connections" =
STRING:
NET-SNMP-EXTEND-MIB::nsExtendOutputFull."443connections" =
STRING:
NET-SNMP-EXTEND-MIB::nsExtendOutNumLines."443connections" =
INTEGER: 1
NET-SNMP-EXTEND-MIB::nsExtendResult."443connections" = INTEGER: 3
NET-SNMP-EXTEND-MIB::nsExtendOutLine."443connections".1 = STRING:

```

Note que o valor de *NET-SNMP-EXTEND-MIB::nsExtendResult."443connections"* = *INTEGER: 3* é o resultado da execução do processo que mostra para nós o valor de saída do processo executado. Ao rodar o comando com a flag **-On** obtemos os valores dos OID's.

```

caetano@ibm4381 ~$ snmpwalk -v 2c -c e23D8s129i4fmsd12 localhost
NET-SNMP-EXTEND-MIB::nsExtendObjects -On

```

Com isso, validamos a criação de um script que estende a MIB. Agora, como um dos requisitos é criar um objeto gerenciável no ramo experimental da MIB, vamos definir esse objeto no arquivo */usr/share/snmp/mibs/N_CONNECTIONS_ON_443.txt* com o seguinte conteúdo:

```

N_CONNECTIONS_ON_443 DEFINITIONS ::= BEGIN
IMPORTS
experimental FROM SNMPV2-SMI;
numConnections OBJECT-TYPE
SYNTAX Unsigned32
MAX-ACCESS read_only
STATUS mandatory
::= { experimental 1 }
END

```

A palavra *Syntax* define o tipo de dado, `N_CONNECTIONS_ON_443` é o nome do objeto, ele é importado do ramo experimental da MIB-2, *Access* define as permissões de acesso do objeto, por exemplo *read-write* ou *read-only*. *Status* define o ciclo de vida. Esse diretório é o diretório que o SNMP carrega as MIBS com MIB DESCRIPTION FILES e pode ser obtido usando o comando:

```
snmptranslate -Dinit_mib .1.3.2>&1 | grep MIBDIR
```

Agora devemos adicionar a seguinte linha no arquivo de configuração do SNMP no agente:

```
extend .1.3.6.1.3.1 N_CONNECTIONS_ON_443 /usr/bin/con-port-443.sh
```

E reiniciamos o serviço usando o comando:

```
sudo systemctl restart snmpd.service
```

Além disso, modificamos o *exit* para um *echo* no script, desse modo o output será um String que é redirecionada para outro OID. Para identificar o OID do objeto gerenciável executamos o comando:

```
caetano@ibm4381 /usr/share/snmp/mibs$ snmpwalk -v 2c -c
e23D8s129i4fmsd12 localhost SNMPv2-SMI::experimental -On
-OUTPUT-----
.1.3.6.1.3.1.1.0 = INTEGER: 1
.1.3.6.1.3.1.2.1.2.20.78.95.67.79.78.78.69.67.84.73.79.78.83.95.7
9.78.95.52.52.51 = STRING: "/usr/bin/con-port-443.sh"
.1.3.6.1.3.1.2.1.3.20.78.95.67.79.78.78.69.67.84.73.79.78.83.95.7
9.78.95.52.52.51 = ""
.1.3.6.1.3.1.2.1.4.20.78.95.67.79.78.78.69.67.84.73.79.78.83.95.7
9.78.95.52.52.51 = ""
.1.3.6.1.3.1.2.1.5.20.78.95.67.79.78.78.69.67.84.73.79.78.83.95.7
9.78.95.52.52.51 = INTEGER: 5
.1.3.6.1.3.1.2.1.6.20.78.95.67.79.78.78.69.67.84.73.79.78.83.95.7
9.78.95.52.52.51 = INTEGER: 1
.1.3.6.1.3.1.2.1.7.20.78.95.67.79.78.78.69.67.84.73.79.78.83.95.7
9.78.95.52.52.51 = INTEGER: 1
.1.3.6.1.3.1.2.1.20.20.78.95.67.79.78.78.69.67.84.73.79.78.83.95.
79.78.95.52.52.51 = INTEGER: 4
.1.3.6.1.3.1.2.1.21.20.78.95.67.79.78.78.69.67.84.73.79.78.83.95.
79.78.95.52.52.51 = INTEGER: 1
```

```
.1.3.6.1.3.1.3.1.1.20.78.95.67.79.78.78.69.67.84.73.79.78.83.95.7
9.78.95.52.52.51 = STRING: "28"
.1.3.6.1.3.1.3.1.2.20.78.95.67.79.78.78.69.67.84.73.79.78.83.95.7
9.78.95.52.52.51 = STRING: "28"
.1.3.6.1.3.1.3.1.3.20.78.95.67.79.78.78.69.67.84.73.79.78.83.95.7
9.78.95.52.52.51 = INTEGER: 1
.1.3.6.1.3.1.3.1.4.20.78.95.67.79.78.78.69.67.84.73.79.78.83.95.7
9.78.95.52.52.51 = INTEGER: 0
.1.3.6.1.3.1.4.1.2.20.78.95.67.79.78.78.69.67.84.73.79.78.83.95.7
9.78.95.52.52.51.1 = STRING: "28"
```

E guardamos o valor de:

- **.1.3.6.1.3.1.4.1.2.20.78.95.67.79.78.78.69.67.84.73.79.78.83.95.79.78.95.52.52.51.1**

Lembrando que **.1.3.6.1.3** é o identificador de **.iso.org.dod.internet.experimental**. Agora basta configurar este item de monitoramento da ferramenta de gerência de redes (*Zabbix*). Adicionamos também na **Cláusula 13.** do contrato um item novo que diz respeito ao monitoramento deste objeto.

12.2. Configuração no Zabbix do item estendido

Cadastramos no host Notebook2, no *Zabbix*, um monitoramento de item SNMP conforme a figura abaixo:

* Name

Type

* Key

Type of information

* Host interface

* SNMP OID

Units

* Update interval

Custom intervals

Type	Interval	Period	Action
<input checked="" type="checkbox"/> Flexible <input type="checkbox"/> Scheduling	50s	1-7,00:00-24:00	Remove

[Add](#)

* History storage period

* Trend storage period

Value mapping

Populates host inventory field

Description

Enabled ☒

Latest data

Figura 28. Configuração do Item novo no Zabbix.

O Zabbix possui uma ferramenta para testar a obtenção de dados via protocolo SNMP, basta definirmos a interface de rede, a porta, a versão do protocolo, a comunidade (no caso do protocolo SNMPv2) e executamos um teste para ver se o valor está sendo recebido pelo host gerente, conforme a figura 29:

Test item

Get value from host
☒

* Host address
192.168.178.211

Port
161

SNMP version
SNMPv2

* SNMP community
e23D8s129i4fmsd12

Proxy
(no proxy)

Value
0

Time
now

Not supported

Previous value

Prev. time

End of line sequence
LF
CRLF

Result
Result converted to Numeric (unsigned)
0

Get value and test

Cancel

Get value

Figura 29. Execução do Teste no Zabbix.

12.3. Modificação do Contrato

Na **Cláusula 13.** do contrato foi adicionado um item (**Item 6**) que diz respeito ao monitoramento deste objeto, o número de conexões ativas na porta 443, a métrica diz que esse número não pode ser maior que 10. Foi modificado o contrato e essa métrica será monitorada junto com outras 5 métricas neste trabalho.

13. MONITORAMENTO DAS MÉTRICAS DO SLA

RESUMO DAS MÉTRICAS

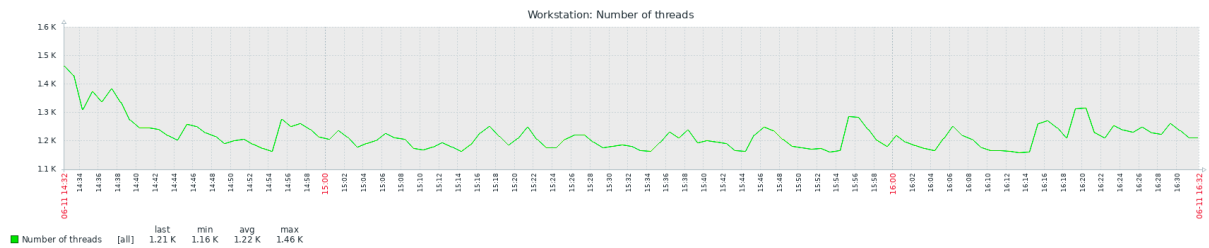
MÉTRICA	STATUS
Cláusula 13. Item 1	VIOLADA
Cláusula 13. Item 2	VIOLADA
Cláusula 13. Item 3	RESPEITADA
Cláusula 13. Item 4	RESPEITADA
Cláusula 13. Item 5	RESPEITADA
Cláusula 13. Item 6	VIOLADA

Tabela 2. Representação gráfica das violações do SLA.

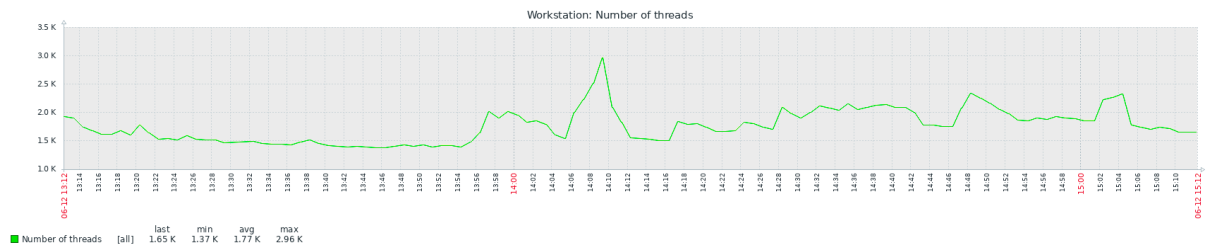
13.1. Número de Threads

Cláusula 13. Item 1. O número de Threads em Workstations não deve ultrapassar 2000.

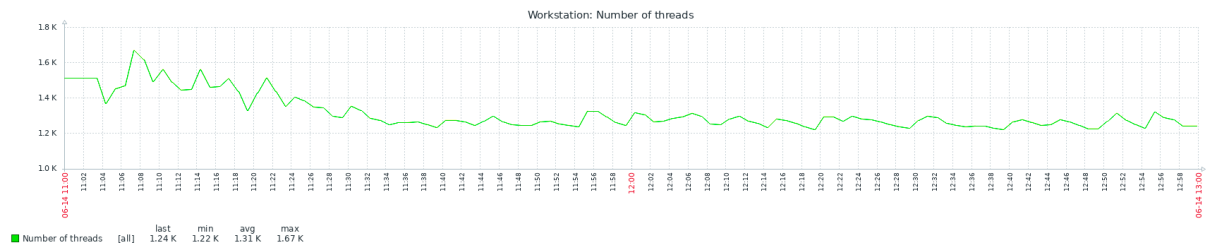
Nessa parte será monitorado o número de Threads no host Workstation, a cláusula do SLA determina que esse número não deve ultrapassar 2000. Percebemos que nas 3 primeiras medições e na quinta medição, o número médio de threads foram aproximadamente 1200 e os níveis do SLA foram respeitados, na quarta medição, foi um dia de uso mais intenso no host e



4- Dia 12/06/2022 13h-15h



5- Dia 14/06/2022 11h-13h



13.2. Uso da Memória RAM

Cláusula 13. Item 2. A utilização da memória host Workstation não pode ultrapassar 90%.

Nessa parte será monitorado o uso da memória RAM no host Workstation, a cláusula do SLA determina que esse número não deve ultrapassar 90% da memória total. Percebemos que na primeira medição houve pouca utilização, cerca de 18% na média. Na segunda medição a média foi de 19% de uso da RAM total. Na terceira medição, o número baixou para 16%. Na quarta medição, houve um uso mais intenso do host durante o tempo monitorado e a RAM chegou até 48% de utilização (dia 12/06, por volta das 14h). Na quinta medição a média foi de cerca de 20% de uso.

Intervalo de Atualização: 1 minuto.

Topologia Gerente \Leftarrow Agente:

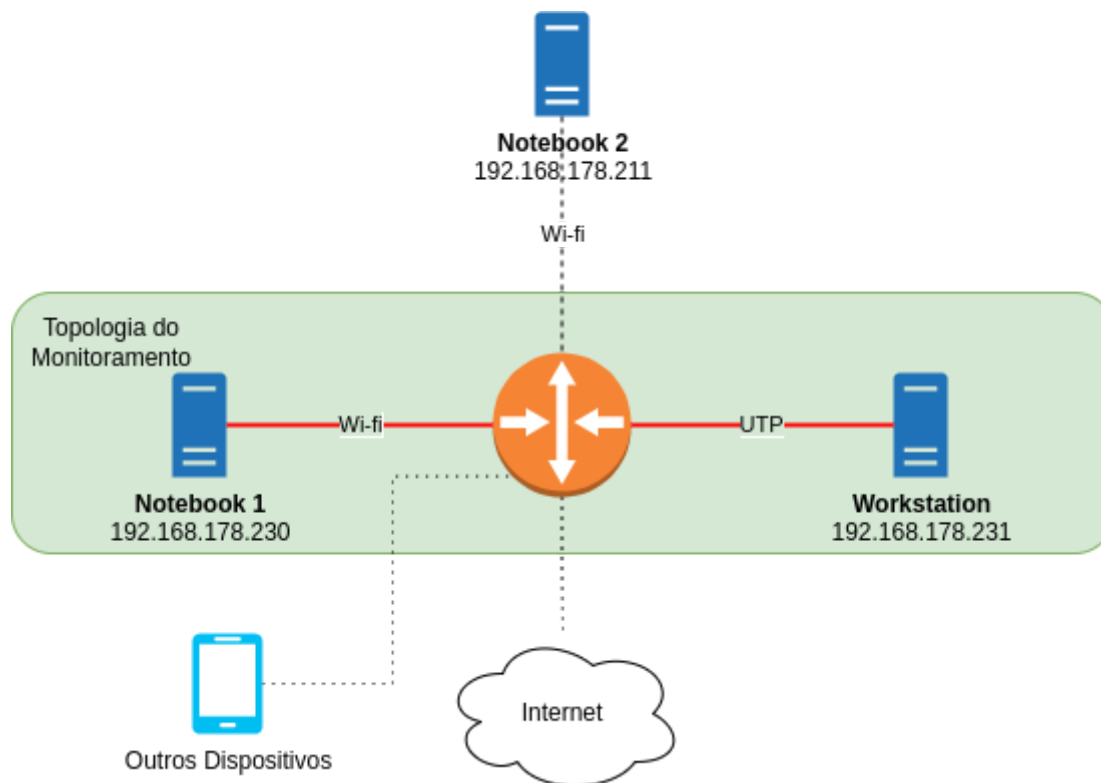
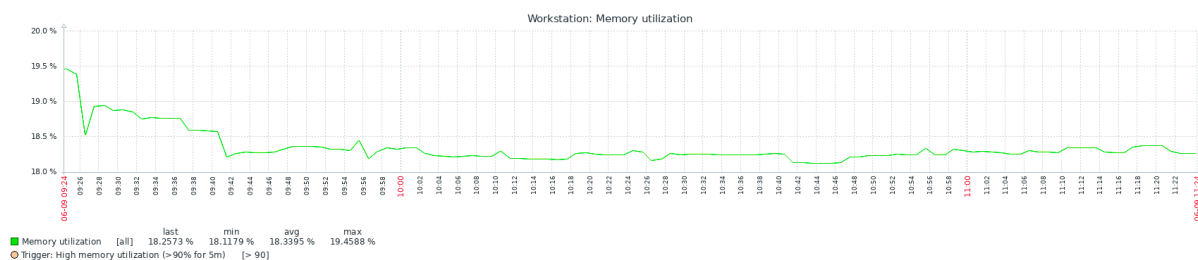
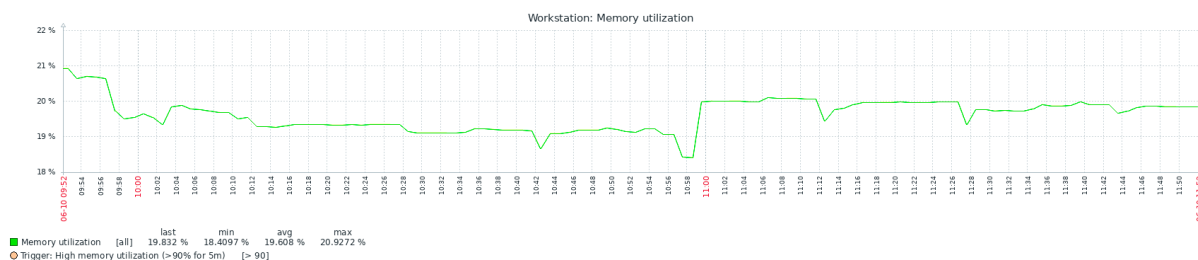


Figura 31. Topologia Notebook 1 (Gerente) ⇌ Workstation (Agente).

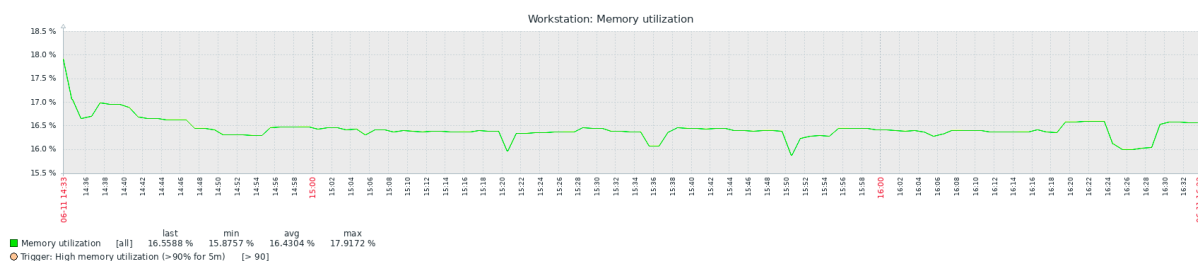
1- Dia 09/06/2022 09h-11h



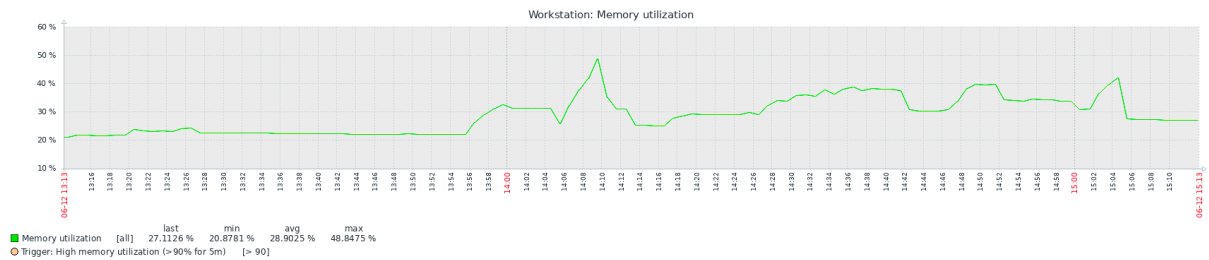
2- Dia 10/06/2022 09h-11h



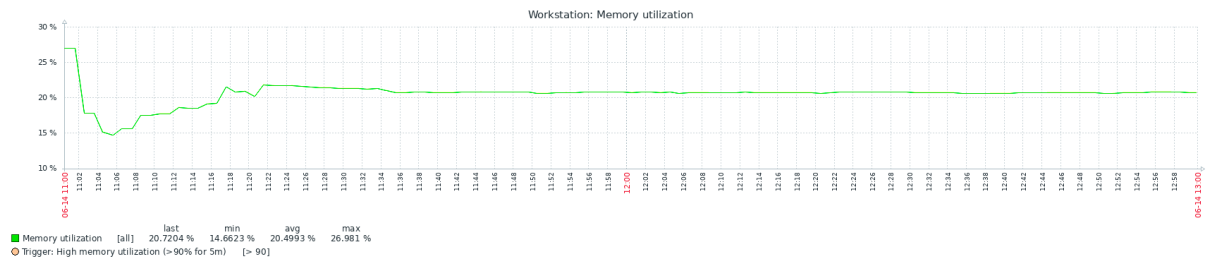
3- Dia 11/06/2022 14h-16h



4- Dia 12/06/2022 13h-15h



5- Dia 14/06/2022 11h-13h



13.3. Tráfego na Interface de Rede

Cláusula 13. Item 3. A taxa de transferência da interface de rede do Notebook2 não deve ultrapassar 10Mbps de download e/ou upload.

Esse monitoramento mede a taxa de transferência da interface de rede Wi-fi do Notebook2, que está conectado na topologia abaixo. Na primeira medição, o número máximo da taxa de transferência foi 474Kbps para dados recebidos e 74Kbps para dados enviados. Na segunda medição, o número máximo da taxa de transferência foi 697Kbps para dados recebidos e 102Kbps para dados enviados. Na terceira medição, o número máximo da taxa de transferência foi 47Kbps para dados recebidos e 5Kbps para dados enviados. Na quarta medição, onde foi executado um **teste de tráfego (Iperf3)** onde o host envia dados para o servidor, o número máximo da taxa de transferência foi 189Kbps para dados recebidos e 9.12Mbps para dados enviados, quase atingindo o limite do SLA. Na quinta medição, o número máximo da taxa de transferência foi 2.85Mbps para dados recebidos e 91.38Kbps para dados enviados.

Intervalo de Atualização: 3 minutos.

Topologia Gerente \Leftarrow Agente:

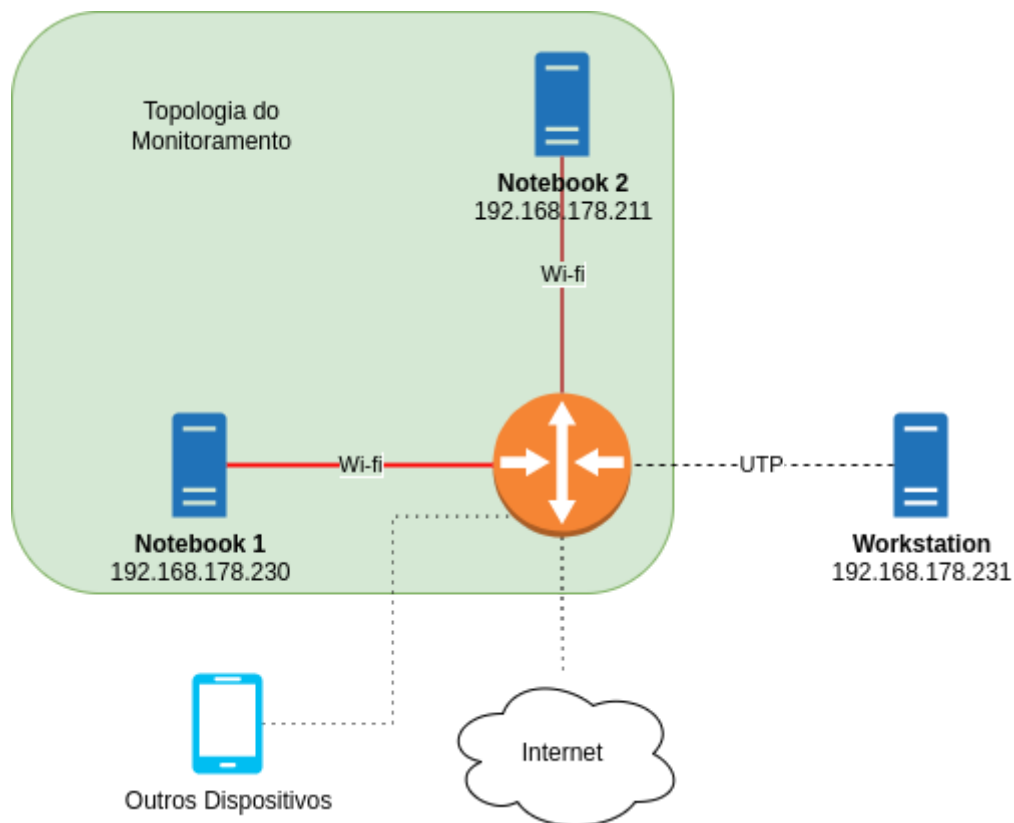
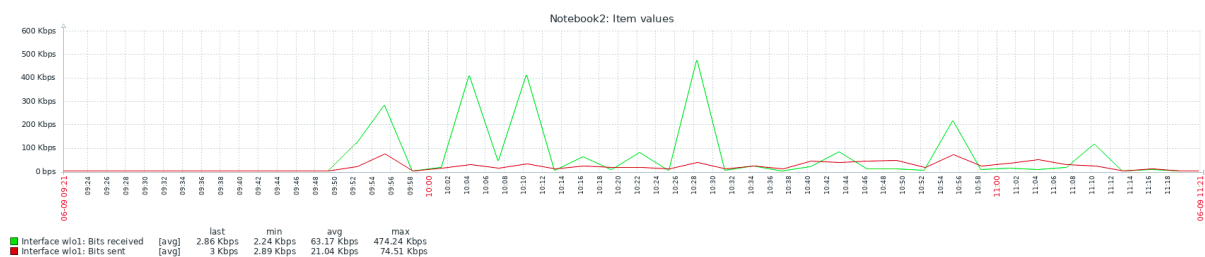
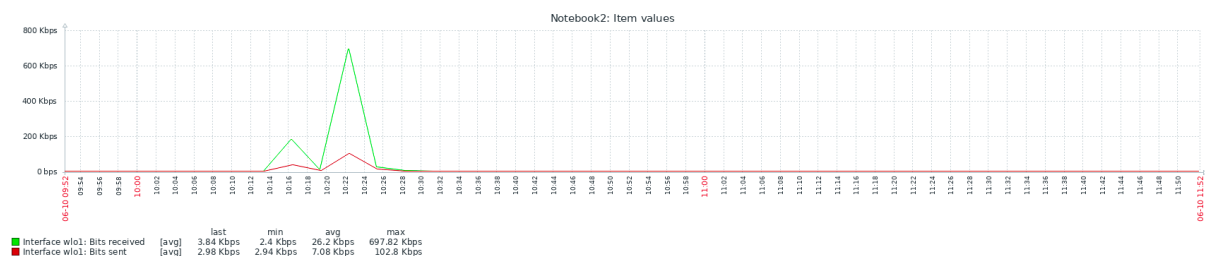


Figura 32. Topologia Notebook 1 (Gerente) \approx Notebook 2 (Agente).

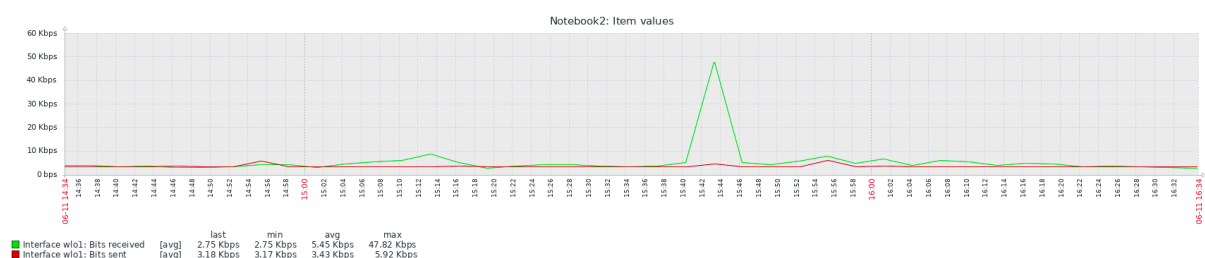
1- Dia 09/06/2022: 09h-11h



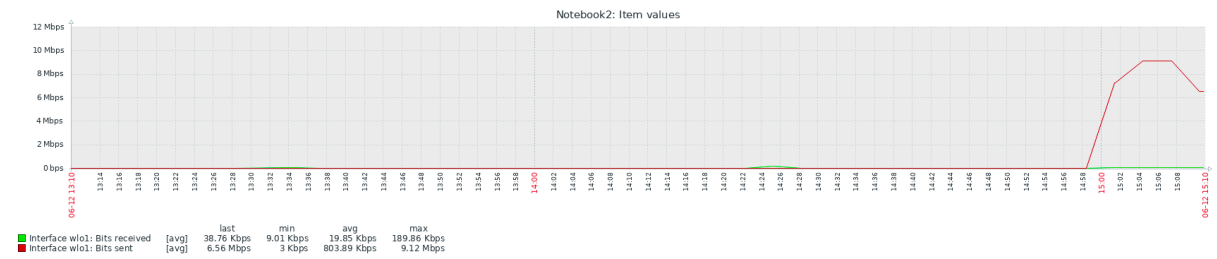
2- Dia 10/06/2022 09h-11h



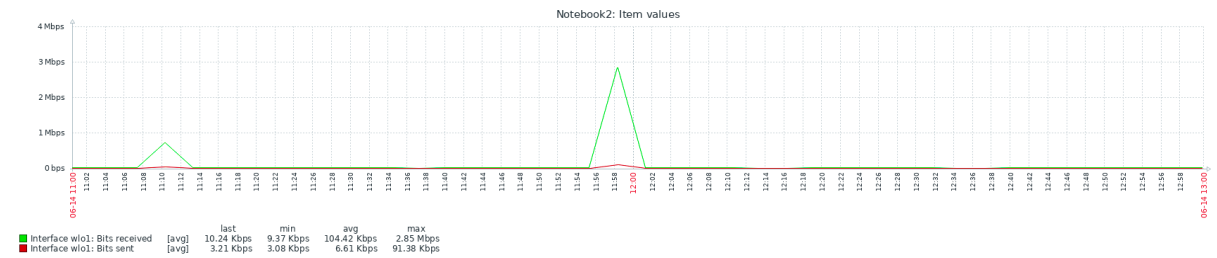
3- Dia 11/06/2022 14h-16h



4- Dia 12/06/2022 13h-15h



5- Dia 14/06/2022 11h-13h



13.4. Disponibilidade do Servidor

Cláusula 13. Item 4. O host gerente não pode ter o uptime zerado durante o tempo monitorado.

Esse monitoramento mede a disponibilidade do servidor na rede, onde é medido o *uptime*, do Notebook1, que hospeda o serviço do Zabbix. Em nenhuma das medições o *uptime* foi zerado, ou seja, em nenhum momento o host ficou indisponível, dessa forma, o limite do SLA foi respeitado.

Intervalo de Atualização: 30 segundos.

Topologia Gerente \rightleftharpoons Agente:

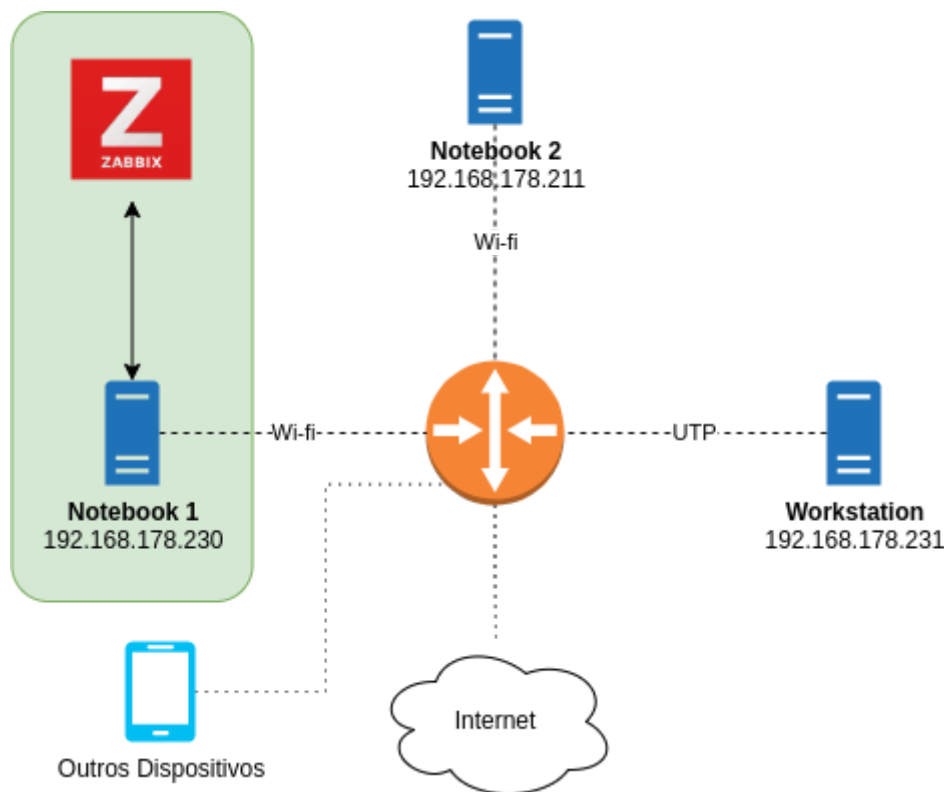
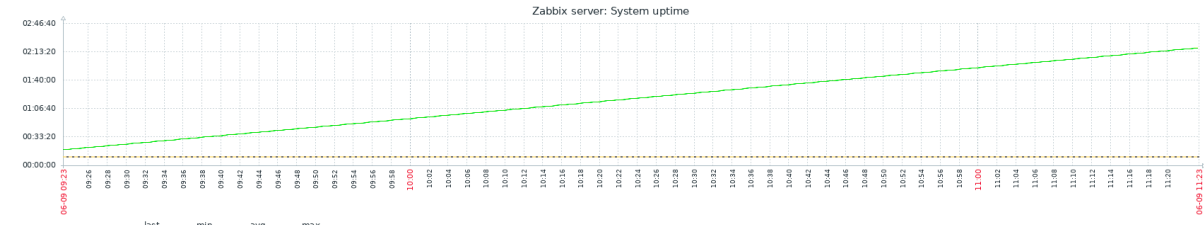
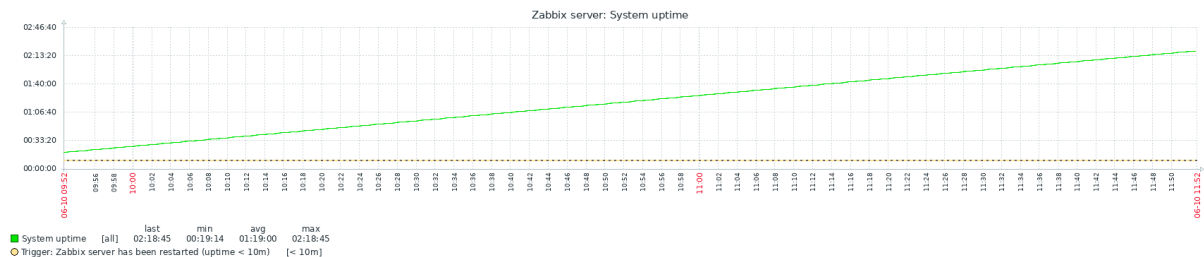


Figura 33. Topologia Notebook 1 (Gerente) \rightleftharpoons Zabbix Server (Local).

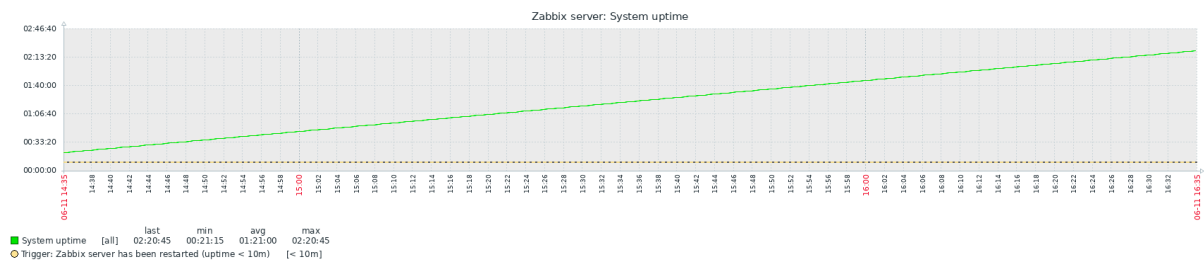
1- Dia 09/06/2022 09h-11h



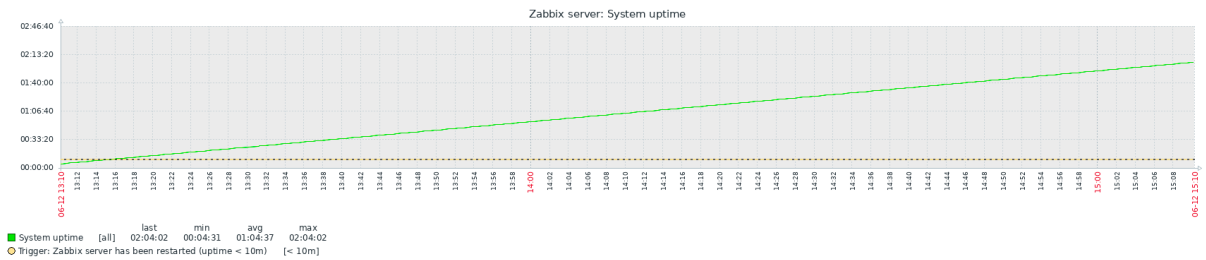
2- Dia 10/06/2022 09h-11h



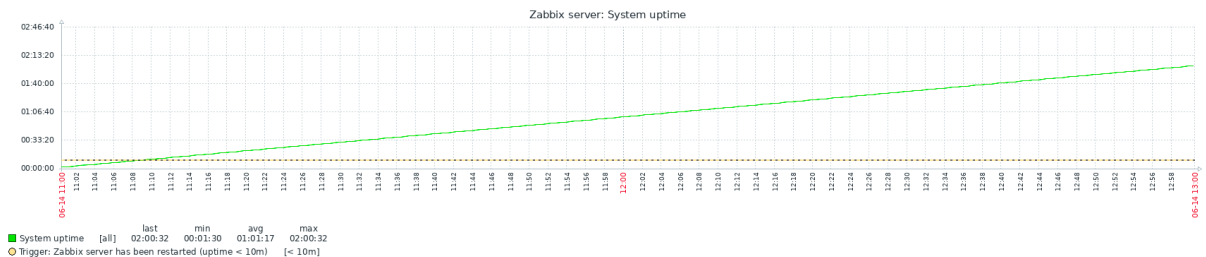
3- Dia 11/06/2022 14h-16h



4- Dia 12/06/2022 13h-15h



5- Dia 14/06/2022 11h-13h



13.5. Número de Inodes

Cláusula 13. Item 5. O número de Inodes disponível no host gerente não pode ser menor que 90%.

Esse monitoramento mede o número de Inodes disponíveis no host gerente em porcentagem. Em todas as medições, o número não foi menor que 95% de Inodes disponíveis, ou seja, em nenhuma medição a métrica do SLA foi violada.

Intervalo de Atualização: 1 minuto.

Topologia Gerente \rightleftharpoons Agente:

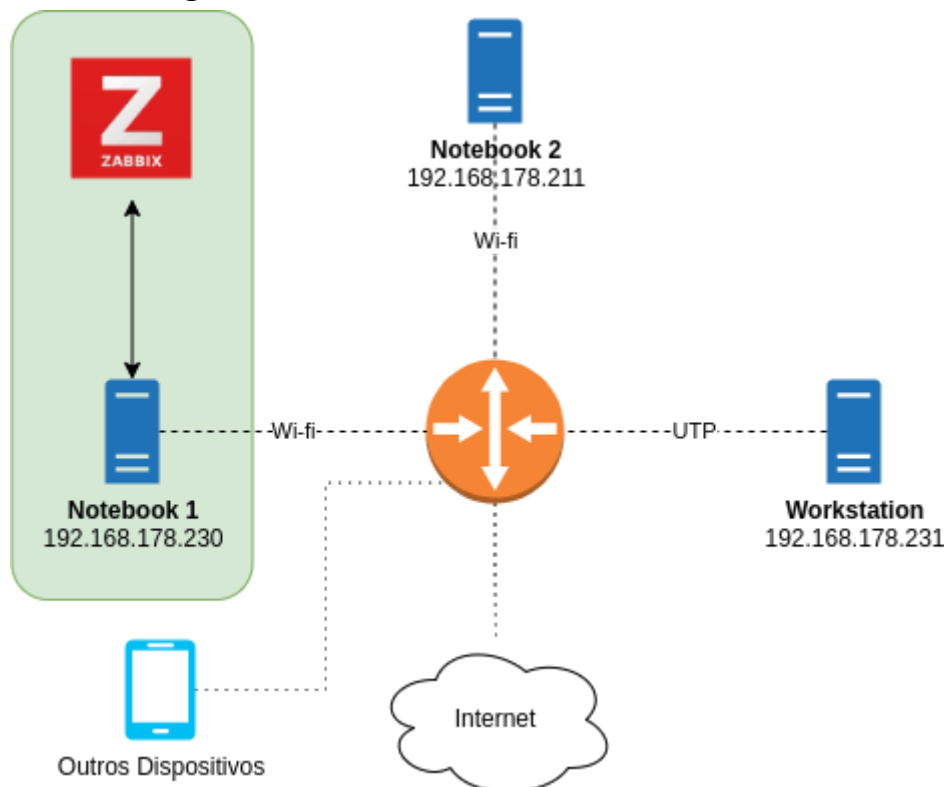
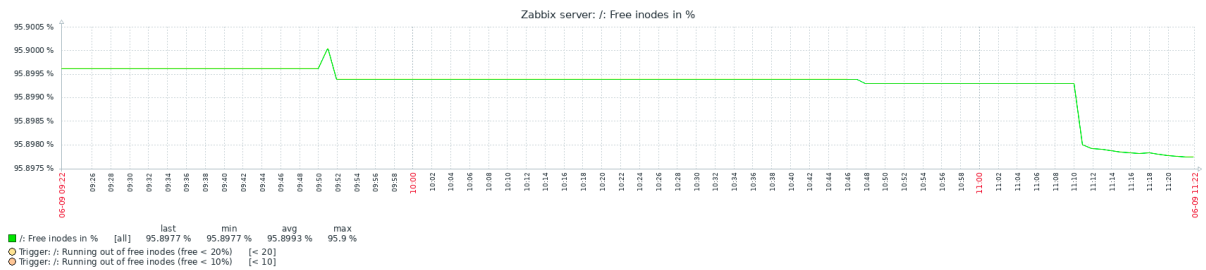
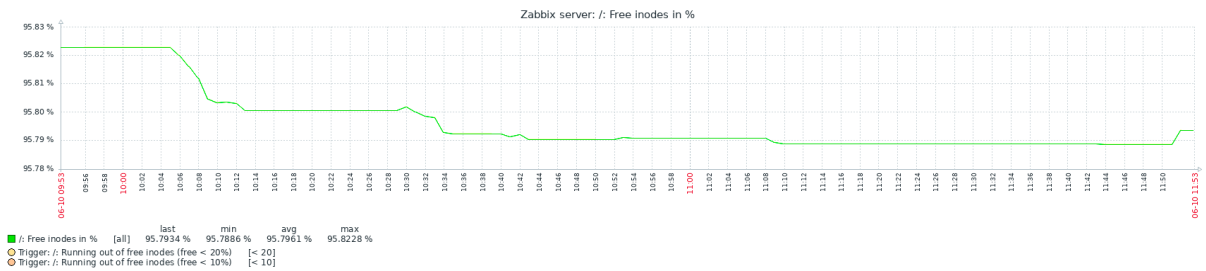


Figura 34. Topologia Notebook 1 (Gerente) \rightleftharpoons Zabbix Server (Local).

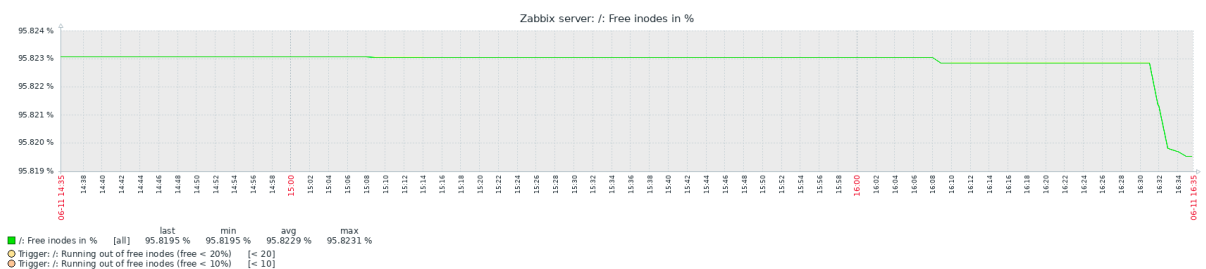
1- Dia 09/06/2022 09h-11h



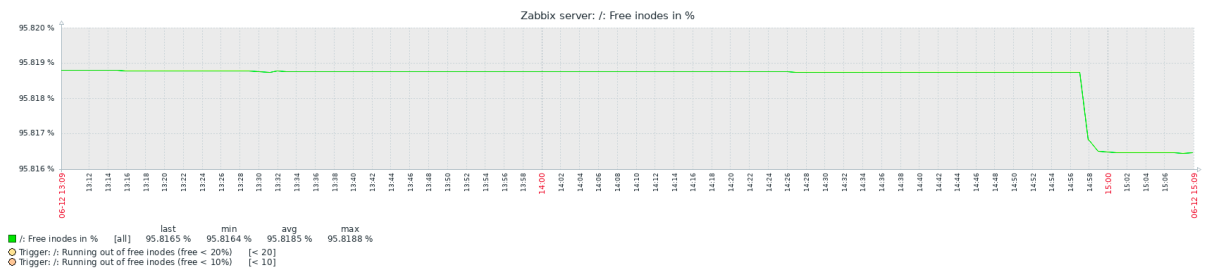
2- Dia 10/06/2022 09h-11h



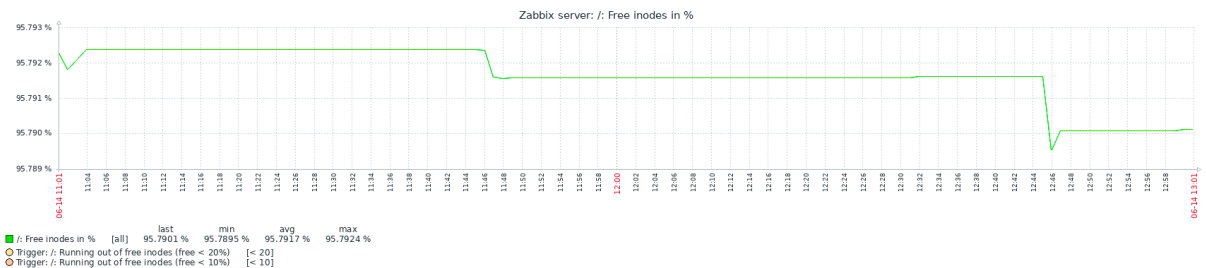
3- Dia 11/06/2022 14h-16h



4- Dia 12/06/2022 13h-15h



5- Dia 14/06/2022 11h-13h



13.6. Número de conexões na porta 443 (MIB Estendida)

Cláusula 13. Item 6. O número de conexões ativas na porta 443 do host Notebook2 não pode ser maior que 10.

Esse monitoramento mede o número de conexões ativas na porta 443, através do objeto estendido na MIB, explicado anteriormente. Nas medições 1,4 e 5 o limite de 10 conexões do SLA foi violado, nos horários 11h04m, 11h08m e 11h02m, respectivamente. Na medição 1 houve um uso intenso do protocolo TLS chegando a até 191 conexões ativas.

Intervalo de Atualização: 1 minuto.

Topologia Gerente \rightleftharpoons Agente:

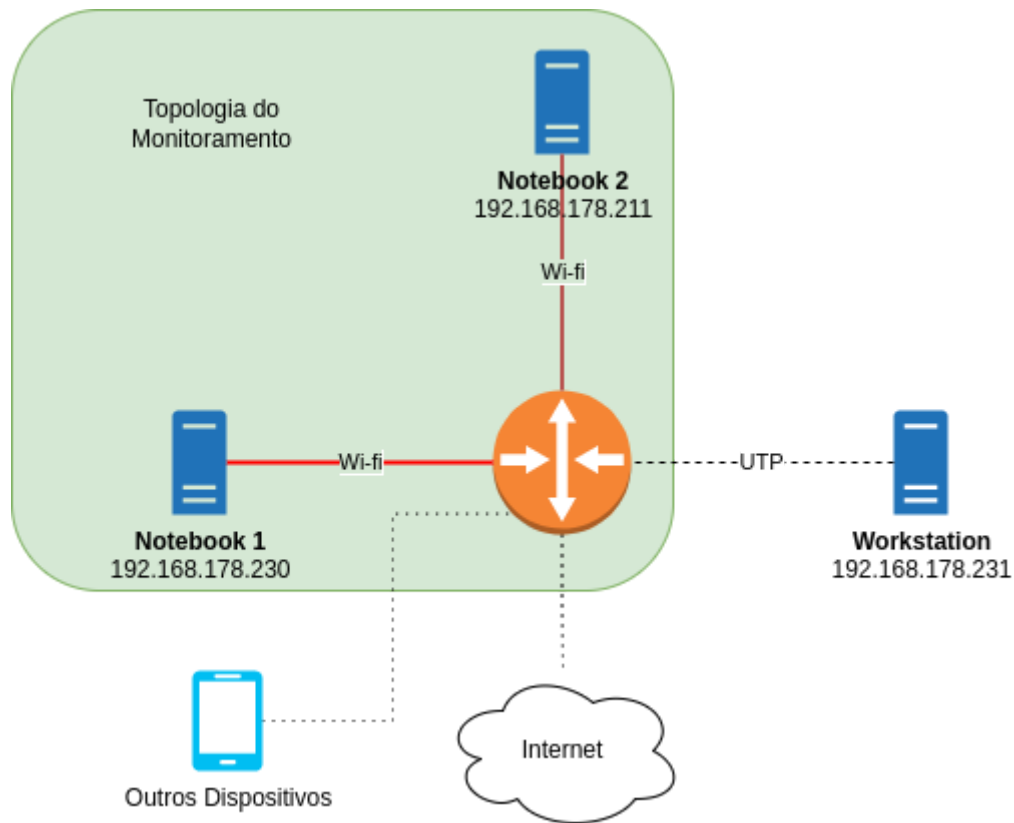
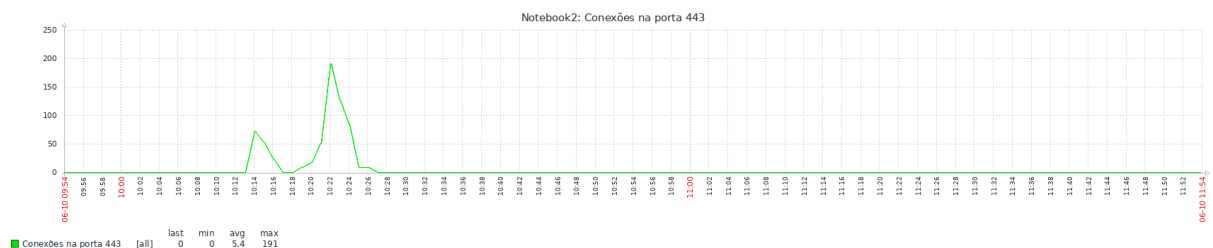


Figura 35. Topologia Notebook 1 (Gerente) \rightleftharpoons Notebook 2 (Agente).

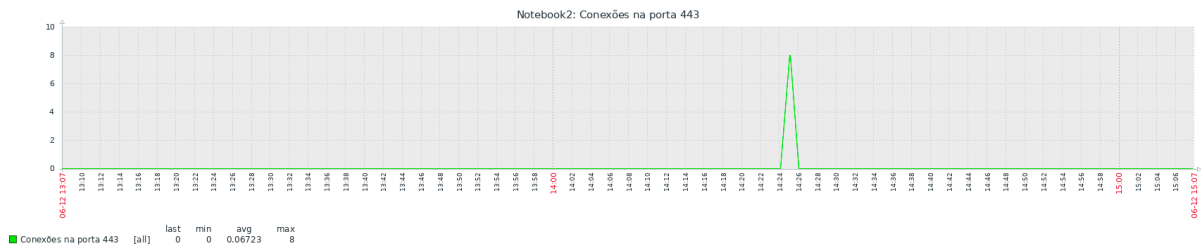
1- Dia 10/06/2022 09h-11h



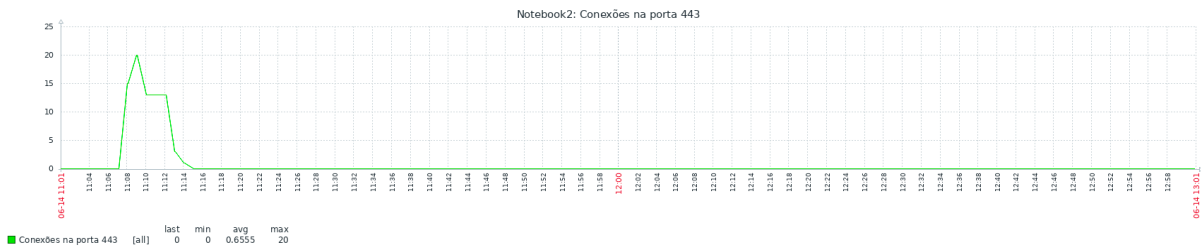
2- Dia 11/06/2022 14h-16h



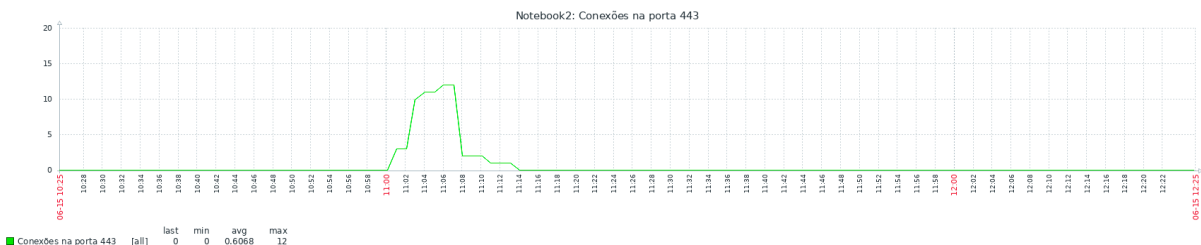
3- Dia 12/06/2022 13h-15h



4- Dia 14/06/2022 11h-13h



5- Dia 15/06/2022 10h-12h



13.6.1 Wireshark do item SNMP

Como o SNMP foi configurado para usar o protocolo UDP na porta 161, começamos a capturar o tráfego de rede nessa porta e executamos o seguinte comando:

```
snmpget -v 2c -c e23D8s129i4fmsd12 192.168.178.211  
.1.3.6.1.3.1.4.1.2.20.78.95.67.79.78.78.69.67.84.73.79.78.83.95.79.78.95.52.52.51.1
```

A resposta do comando que obtemos é a seguinte:

```
iso.3.6.1.3.1.4.1.2.20.78.95.67.79.78.78.69.67.84.73.79.78.83.95.79.78.95.52.52.51.1 =  
STRING: "0"
```

E o resultado da captura de tráfego é o da figura abaixo, note que está destacado em rosa o resultado do comando SNMP executado anteriormente.

udp.port == 161						
No.	Time	Source	Destination	Protocol	Length	Info
279	10.055277703	192.168.178.230	192.168.178.211	SNMP	133	get-request 1.3.6.1.2.1.25.1.1.0 1.3.6.1.3.1.4.1.2.20.78.95.6...
284	10.096407050	192.168.178.211	192.168.178.230	SNMP	137	get-response 1.3.6.1.2.1.25.1.1.0 1.3.6.1.3.1.4.1.2.20.78.95...
294	11.122780972	192.168.178.230	192.168.178.211	SNMP	135	get-request 1.3.6.1.4.1.2021.11.54.0 1.3.6.1.4.1.2021.11.59.0...
296	11.130299787	192.168.178.211	192.168.178.230	SNMP	135	get-response 1.3.6.1.4.1.2021.11.54.0 1.3.6.1.4.1.2021.11.59...
297	11.130841450	192.168.178.230	192.168.178.211	SNMP	135	get-request 1.3.6.1.4.1.2021.11.61.0 1.3.6.1.4.1.2021.11.53.0...
298	11.132347204	192.168.178.230	192.168.178.211	SNMP	135	get-request 1.3.6.1.4.1.2021.4.3.0 1.3.6.1.4.1.2021.11.64.0 1...
299	11.132894792	192.168.178.230	192.168.178.211	SNMP	133	get-request 1.3.6.1.4.1.2021.4.6.0 1.3.6.1.2.1.1.3.0 1.3.6.1...
300	11.143348542	192.168.178.211	192.168.178.230	SNMP	135	get-response 1.3.6.1.4.1.2021.11.61.0 1.3.6.1.4.1.2021.11.53...
301	11.143819701	192.168.178.230	192.168.178.211	SNMP	119	get-request 1.3.6.1.4.1.2021.11.65.0 1.3.6.1.4.1.2021.11.66.0...
302	11.154878524	192.168.178.211	192.168.178.230	SNMP	135	get-response 1.3.6.1.4.1.2021.4.3.0 1.3.6.1.4.1.2021.11.64.0 ...
303	11.154915303	192.168.178.211	192.168.178.230	SNMP	136	get-response 1.3.6.1.4.1.2021.4.6.0 1.3.6.1.2.1.1.3.0 1.3.6.1...
304	11.155462353	192.168.178.230	192.168.178.211	SNMP	87	getBulkRequest 1.3.6.1.4.1.2021.10.1.2
305	11.155528814	192.168.178.211	192.168.178.230	SNMP	87	getBulkRequest 1.3.6.1.2.1.25.3.3.1.1
306	11.156932622	192.168.178.211	192.168.178.230	SNMP	119	get-response 1.3.6.1.4.1.2021.11.65.0 1.3.6.1.4.1.2021.11.66...
307	11.160221276	192.168.178.211	192.168.178.230	SNMP	87	get-response 1.3.6.1.4.1.2021.10.1.2
308	11.165363545	192.168.178.211	192.168.178.230	SNMP	87	get-response 1.3.6.1.2.1.25.3.3.1.1
714	24.325857945	192.168.178.230	192.168.178.211	SNMP	118	get-request 1.3.6.1.3.1.4.1.2.20.78.95.67.79.78.78.69.67.84.7...
721	24.348615338	192.168.178.211	192.168.178.230	SNMP	119	get-response 1.3.6.1.3.1.4.1.2.20.78.95.67.79.78.78.69.67.84...

Figura 36. Captura de Tráfego na porta 161, protocolo de transporte UDP.

Ao analisar o pacote 721:

Frame 721: 119 bytes on wire (952 bits), 119 bytes captured (952 bits) on interface wlp0s20f3, id 0 Ethernet II, Src: IntelCor_fa:32:91 (b4:b6:76:fa:32:91), Dst: IntelCor_ee:81:bc (dc:1d:a1:ee:81:bc) Internet Protocol Version 4, Src: 192.168.178.211, Dst: 192.168.178.230 User Datagram Protocol, Src Port: 161, Dst Port: 53415 Simple Network Management Protocol	
Version: v2c (1)	community: e2308s12914fmsd12
data: get-response (2)	
get-response	
request-id: 1384611805	
error-status: noError (0)	
error-index: 0	
variable-bindings: 1 item	
Object Name: 1.3.6.1.3.1.4.1.2.20.78.95.67.79.78.78.69.67.84.73.79.78.83.95.79.78.95.52.52.51.1: 30	
[Response To: 714] [Time: 0.022757393 seconds]	

Figura 37. Pacote 721, resposta do pedido SNMP Get.

Visualizamos que a resposta (pacote 721) é uma *OctetString* que corresponde de valor hexadecimal 30 que, por sua vez, em ASCII é decodificado para o caractere “0”, conforme visualizamos na resposta do comando.

REFERÊNCIAS

- [1] BESTMONITORINGTOOLS. How to Install Zabbix 6.0 on Ubuntu 20.04 [Step-by-Step]. <https://bestmonitoringtools.com/how-to-install-zabbix-server-on-ubuntu/#Step_1_Install_Zabbix_server_frontend_and_agent>. Acesso em: 02 de mai. de 2022.
- [2] CEZAR, Matei. How to Install and Configure Zabbix Agents on Remote Linux – Part 3. 2021. Disponível em: <tecmint.com/install-and-configure-zabbix-agents-on-centos-redhat-and-debian/>. Acesso em: 24 de mai. de 2022.
- [3] AIT Inc. How to Setup Zabbix Agent on Windows. 2017. Disponível em: <<https://www.ait.com/tech-corner/11491-how-to-setup-zabbix-agent-on-windows#:~:text=Go%20to%20the%20Zabbix%20web,OS%20Windows%20and%20click%20Add.>>. Acesso em: 24 de mai. de 2022.
- [4] GOLINUXCLOUD. 6 commands to check and list active SSH connections in Linux. 2022. Disponível em: <<https://www.golinuxcloud.com/list-check-active-ssh-connections-linux/>>. Acesso em: 09 de jun. de 2022.

- [5] REDHAT. Extending Net-SNMP. 2022. Disponível em: <https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/deployment_guide/sect-system_monitoring_tools-net-snmp-extending>. Acesso em: 09 de jun. de 2022.
- [6] KHAN, Ahmed. Extending the SNMP Agent. Custom Script, Custom MIB, Custom Enterprise OID. 2021. Disponível em: <<https://github.com/ahmednawazkhan/guides/blob/master/snmp/creating-custom-mib.md>>. Acesso em: 09 de jun. de 2022.